Facultad de Ingeniería

Ingeniería de Redes y Comunicaciones

Programa Especial de Titulación:

Implementación de una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte

Roberto Jossimar Flores Ayqui

Para optar por el título Profesional de

Ingeniero de Redes y Comunicaciones

Asesor: Laberiano Andrade Arenas

Lima - Perú

2021

Dedicatoria

A mis padres por su incansable, ilimitado apoyo y amor incondicional a lo largo de todas nuestras vidas, por enseñarme a valorar los momentos y cosas de la vida, por sembrar en mi humildad, por sus consejos, porque los amo mucho, por ser hoy lo que somos gracias a ellos.

Agradecimiento

A nuestros asesores y profesores del PET, quienes nos guiaron y orientaron en la elaboración de este ISP, por su paciencia, entrega y vocación plasmada en todos nosotros, agradezco a todas mis amistades que me acompañaron en este reto y siempre trasmitieron sus mejores deseos para lograr este objetivo.

RESUMEN

En la actualidad, de todos los cambios y transformaciones que traerá consigo la pandemia y el estado de emergencia sanitaria ante el COVID-19, reorganizar y determinar patrones laborales como el espacio y las limitaciones en las que laboramos, son algunos de los efectos que más prontamente veremos materializarse. **En este contexto, el teletrabajo es un intérprete muy principal de la transición hacia la nueva normalidad laboral post-coronavirus.**

En el actual informe se procura exponer la problemática a la cual se enfrenta el Hospital de baja complejidad de Vitarte con respecto al teletrabajo y el propósito de implementar una VPN-SSL, la autenticación Multifactor, el acceso a los sistemas, recursos y aplicaciones, y por último el monitoreo y auditoría, todo esto de forma eficiente y segura. Frente a esto se brinda una propuesta de solución basada en la implementación de dispositivos y tecnologías de la marca Fortinet, la cual cuenta con equipos óptimos y diseñados para lograr el objetivo.

La estrategia de solución aplicada se basó en la metodología PPDIOO de Cisco la cual mediante sus fases nos permitió lograr cada objetivo específico y así obtener resultados exitosos.

La conclusión más resaltante que se pretende evidenciar con el presente ISP es demostrar que mediante la implementación de una VPN-SSL con la seguridad apropiada se simplificará y logrará poner en marcha en su totalidad la modalidad de Teletrabajo, sin ser necesaria la asistencia física del colaborador en sitio. El trabajo remoto es una práctica laboral la cual favorece a muchas personas compensando sus tareas profesionales y personales, convoca a la sociedad a adaptarse a estos cambios explotando al máximo las nuevas tecnologías.

Palabras claves: VPN, autenticación, acceso, Multifactor, monitoreo.

ABSTRACT

At present, of all the changes and transformations that the pandemic and the state of health emergency in the face of COVID-19 will bring with it, reorganizing and determining work patterns such as the space and limitations in which we work, are some of the effects that most we will soon see it materialize. **In this context, teleworking is a very main interpreter of the transition towards the new post-coronavirus work normality.**

The current report seeks to expose the problems faced by the Low Complexity Hospital of Vitarte with respect to teleworking and the purpose of implementing a VPN-SSL, Multifactor authentication, access to systems, resources and applications, and finally monitoring and auditing, all this efficiently and safely. Against this, a solution proposal is provided based on the implementation of Fortinet brand devices and technologies, which has optimal equipment designed to achieve the objective.

The solution strategy applied was based on Cisco's PPDIOO methodology, which through its phases allowed us to achieve each specific objective and thus obtain successful results.

The most outstanding conclusion that is intended to be evidenced with this ISP is to demonstrate that by implementing a VPN-SSL with the appropriate security, the Teleworking modality will be simplified and will be able to fully implement, without requiring the physical assistance of the collaborator In place. Remote work is a work practice that favors many people by compensating their professional and personal tasks, calls on society to adapt to these changes by exploiting new technologies to the maximum.

Keywords: VPN, authentication, access, multi-factor, monitoring.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

INTRODUCCION

La implementación de una VPN-SSL en el Hospital de Vitarte es muy primordial y necesaria ya que facilita la conexión, comunicación y transporte seguro de la información, siempre y cuando se considere la seguridad y el integro viaje de los datos mediante esta conexión.

No obstante, el Hospital de Vitarte no cuenta con una conexión VPN-SSL como opción de teletrabajo ante el estado de emergencia sanitaria para los trabajadores de dicha entidad. Actualmente este tipo de conexiones remotas se realizan por medios no tan seguros y de forma independiente, lo cual puede abrir brechas de seguridad o ser un canal fácil de fuga de información. Como resultado no se tiene una conexión directa a los sistemas, recursos o aplicaciones de la red del Hospital, esto trae como consecuencia el incumplimiento a tiempo de las actividades asignadas por cada Unidad para los trabajadores de la entidad.

Además, es de suma importancia la autenticación de los usuarios en dicha conexión a través de la VPN-SSL por ello se añadirá una capa adicional de seguridad como método de doble factor de autenticación, la cual será registrada y sincronizada mediante correo electrónico personal, generando así un código con la finalidad de validar y autorizar la autenticidad de estas conexiones (el primer factor deberá ser el usuario y contraseña del dominio y el segundo factor el código generado por el Token como aplicativo previamente instalado). Así, se crea una capa extra de defensa basada en múltiples barreras de paso que dificulta en gran medida el acceso a una persona no autorizada. La autenticación Multifactor (MFA) es un aliado para los usuarios y para la empresa desde un punto de vista global la cual procura que únicamente estos se encuentren pertinentemente autorizados para alcanzar la información de forma segura.

Por último, se podrán registrar eventos y generar trazabilidad sobre las operaciones que realizan los trabajadores remotos en los sistemas de información como parte de un monitoreo correcto y de gran ayuda para que el Teletrabajo sea exitoso.

La propuesta de implementar una VPN-SSL será aplicada para facilitar el trabajo remoto para los distintos grupos de trabajadores del Hospital de Baja Complejidad de Vitarte en la actual coyuntura que cruzamos.

CAPITULO 1

ASPECTOS GENERALES

1.1. Definición del Problema

1.1.1. Descripción del Problema

Debido al estado de emergencia sanitaria a nivel nacional ante el COVID-19 se han manifestado recientemente estilos de trabajo a través de medios tecnológicos como lo menciona y es regulado en la Ley N°30036 para el teletrabajo y el trabajo remoto. En este contexto, el Hospital de Vitarte, institución pública como materia de estudio optó por seguir atendiendo a los pacientes aledaños de la población de Vitarte mediante el TELETRABAJO, TELESALUD y TELEMEDICINA.

Los trabajadores no cuentan con una modalidad de conexión remota segura que les permita ingresar directamente a los sistemas, recursos y aplicaciones de la red del Hospital, utilizando así software gratuito de conexión remota como TeamViewer o AnyDesk con el fin de ingresar a las estaciones de trabajo propias de la institución.

Por tal motivo, el problema principal es la carencia de una conexión VPN-SSL que facilite este tipo de interacción, generando retraso, postergación y en algunos casos el incumplimiento a tiempo de las actividades asignadas por cada unidad o servicio del Hospital. Además, los accesos a través de software remoto gratuito tienen un tiempo límite de conexión, ya que para poder usarlos sin límites ni restricciones deberán adquirirse licencias comerciales costosas.

Al realizar este tipo de conexión no existe la autenticación Multifactor, lo cual no proporciona métodos de autenticación robustas y rápidas como factor de disponibilidad. Capa adicional de protección como elemento constructivo de seguridad que se debe considerar e implementar para

obligar a los usuarios a validar su identidad empleando dos o más procedimientos de comprobación antes de llegar a autenticarse. Permitiendo gestionar de forma efectiva la identidad de los trabajadores remotos que se conectaran mediante la VPN-SSL a la red del Hospital de Vitarte.

En consecuencia, no existe un registro o control como rastro de auditoria para estas conexiones, por lo cual la entidad no puede verificar eventos de acceso o generar reportes que registren las actividades o tiempo de servicio de los trabajadores en esta modalidad.

En efecto a lo descrito se puede considerar que es fundamental la implementación de una VPN-SSL con integración de los usuarios del Active Directory (LDAP) a través del Firewall FortiGate utilizando un método de doble factor de autenticación para el acceso a los sistemas y así aplicar la modalidad de teletrabajo en el Hospital de Vitarte.

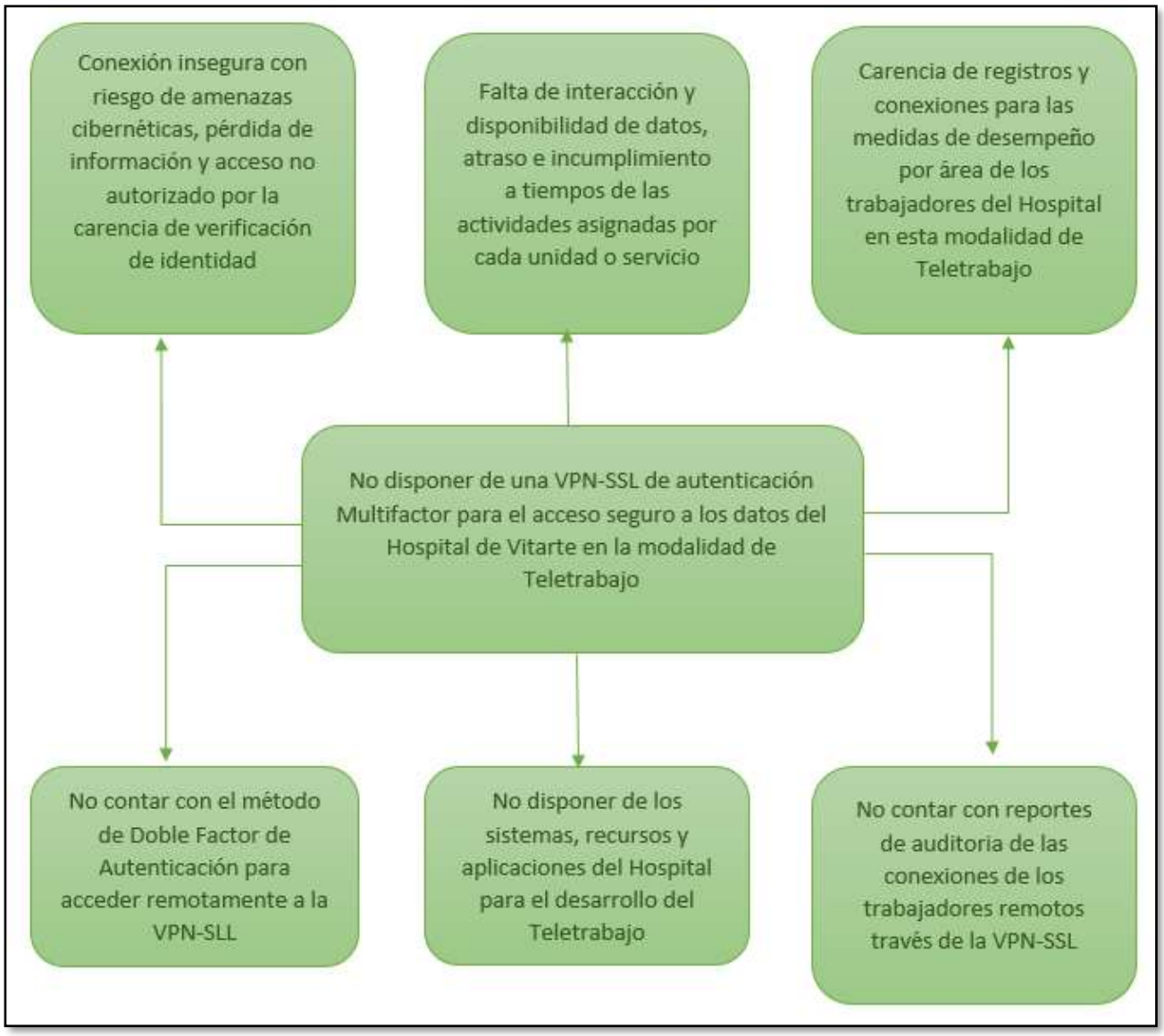


Figura 1. Árbol de problemas

1.1.2. Formulación del Problema

1.1.2.1. Problema General:

¿Es posible la implementación de una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte?

1.1.2.2. Problemas Específicos:

- ¿Es posible implementar el método de Doble Factor de Autenticación para acceder remotamente a la VPN-SSL?
- ¿Es posible la disponibilidad de los sistemas, recursos y aplicaciones alojadas en los servidores del Hospital de Vitarte para el desarrollo del Teletrabajo mediante una VPN-SSL?
- ¿Es posible monitorear y auditar las conexiones de los trabajadores remotos del Hospital de Vitarte mediante la VPN-SSL?

1.2. Definición de objetivos

1.2.1. Objetivo general

Implementar una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte.

1.2.2. Objetivos específicos

- Implementar el método de Doble Factor de Autenticación para acceder remotamente a la VPN-SSL.
- Aplicar la disponibilidad de los sistemas y recursos alojadas en los servidores del Hospital de Vitarte para el desarrollo de la modalidad de Teletrabajo mediante una VPN-SSL.
- Monitorear y auditar las conexiones de los trabajadores remotos del Hospital de Vitarte mediante una VPN-SSL.

1.3. Alcances y limitaciones

1.3.1. Alcances

El alcance de este informe de suficiencia profesional con base a la definición del problema y de acuerdo a los objetivos específicos, propone lo siguiente:

- Mejorar la calidad de atención de los trabajadores ante la implementación de la modalidad de conexión remota segura que les permita ingresar directamente a los sistemas, recursos y aplicaciones del Hospital de Vitarte.
- Clasificar grupos de dominio por cada unidad o servicio para la conexión remota que se llevara a cabo en el horario laborable correspondiente.
- Gestionar la lista de trabajadores según jefatura de cada unidad o servicio y declararla mediante el protocolo LDAP ya configurado y sincronizado en el Firewall FortiGate-100E.

- Asignar token virtual (FortiToken) como método de doble factor de autenticación para cada usuario VPN registrando un correo personal para su activación del mismo y sincronización a través del aplicativo gratuito FortiToken Mobile.
- Generar reportes como monitoreo y auditoria de la conexión de los trabajadores remotos de cada unidad o servicio mediante el Appliance FortiAnalyzer-200D.
- Contar con un plan de contingencia para la conexión VPN-SSL ante algún desperfecto o caída del enlace de Internet contratado por el Hospital de Vitarte, para ello se contará con un enlace secundario Backup disponible para este tipo de incidencias.
- Desarrollar manuales y capacitaciones para las unidades y servicios que contaran con esta modalidad de trabajo remoto, determinando los requisitos necesarios para lograr esta conexión e interacción con las diferentes aplicaciones alojadas en los servidores del Hospital de Vitarte.

1.3.2. Limitaciones

- No Contar con una velocidad moderada de Internet.
- No contar con los planos de las Unidades y Servicios propias de la entidad.
- Por parte del personal, desinterés y temor a las nuevas tecnologías existentes.
- No contar con ningún tipo de documentación del diseño original de la estructura de red existente

1.4. Justificación

El motivo de este informe y su vital importancia, es la implementación de una VPN-SSL en el Hospital de Vitarte, con el fin de que los trabajadores cuenten con este acceso de forma segura.

Además, esta VPN-SSL estará integrada con el Directorio Activo de la organización mediante el protocolo LDAP, permitiendo así establecer niveles de acceso por usuarios o grupos del dominio ya existentes.

El motivo de elección de esta arquitectura, se basa en lograr una conexión segura y confiable. Ya que, para mejorar la autenticación y mantener el acceso seguro a los sistemas a través de esta conexión VPN, el túnel estará encriptado y como capa adicional de seguridad se implementará el método de doble factor de autenticación.

Es decir, cada usuario contará con un Token digital el cual será activado mediante su correo personal, dicho token digital es un aplicativo gratuito que será previamente instalado y configurado en el dispositivo móvil del trabajador, el mismo que genera códigos aleatorios de 6 dígitos cada 60 segundos mejorando la autenticación sin comprometer o vulnerar la identidad.

Finalmente se logrará la interacción y disponibilidad de datos al ingresar a los sistemas por parte del trabajador cumpliendo así sus actividades asignadas por cada unidad, ya que las medidas de desempeño por área serán monitoreadas como parte de una buena auditoría en esta modalidad del Teletrabajo.

Esta propuesta estará basada en la solución tecnológica de la marca Fortinet que será implementada en el Hospital de Vitarte para la modalidad de teletrabajo propuesta ante el estado de emergencia sanitaria producto del COVID-19, priorizando así la continuidad y compromiso del sector salud para la población de Ate-Vitarte, se contará con capacitaciones y manuales para mantener a los trabajadores actualizados de cada cambio o necesidad que se requiera para lograr sus objetivos laborales.

CAPITULO 2

MARCO TEÓRICO

2.1.Fundamento Teórico

2.1.1. Estado del Arte

Tesis de otras universidades y artículos:

En la Universidad Central de Venezuela se sustentó la Tesis **"DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN-SSL) UTILIZANDO EL MÉTODO DE AUTENTICACIÓN LDAP EN UNA EMPRESA PRIVADA"**, por el bachiller Daniela V. Peña en octubre de 2016.

Esta investigación tuvo como finalidad implementar una red privada virtual VPN-SSL integrando la autenticación con el protocolo LDAP en una empresa privada, con el propósito de proteger las conexiones de acceso remoto de forma cifrada garantizando la integridad, confidencialidad y seguridad de los datos. Durante la investigación se abarcaron teorías y documentación de las conexiones utilizadas en la actualidad. También se realizó una serie de comparaciones entre el protocolo SSL con respecto al Ipsec, la configuración de un firewall como intermediario y por último un manual para gestionar la conexión mediante la VPN-SSL. (Peña, 2016)

En la Universidad Autónoma del Perú se sustentó la Tesis **"PROPUESTA DE UNA RED PRIVADA VIRTUAL PARA MEJORAR EL SERVICIO DE COMUNICACIÓN EN**

LAS TIENDAS MASS PARA LA EMPRESA SUPERMERCADOS PERUANOS S.A", por el bachiller Cesar Espinoza Chipane en febrero de 2018.

En este proyecto se tiene como finalidad la propuesta de una solución de red privada virtual enfocada en las tiendas MASS pertenecientes a la empresa Supermercados Peruanos, aplicando la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar) de Cisco Systems que ayudara en cada etapa lograr la propuesta de implementación, este tipo de solución o conexión está más orientada a enlazar o comunicar distintas sucursales geográficamente apartadas todo esto bajo el concepto de una VPN Sitio a Sitio. (Espinoza, 2018)

En la Universidad Nacional de Loja se sustentó la Tesis **"DISEÑO DE UNA VPN PARA EL ACCESO A LAS BASES DE DATOS CIENTIFICAS DE LA UNIVERSIDAD NACIONAL DE LOJA"**, por el bachiller Henry Quezada Lozano en marzo de 2016.

El actual trabajo de titulación se basa en el Diseño de una VPN para la entrada y conexión a las bases de datos de la Universidad de Loja, con el propósito de conseguir una prestación la cual permita a los integrantes de la congregación universitaria ingresar remotamente a los recursos de la red interna de la entidad desde cualquier red externa lejana.. (Quezada, 2016)

En el artículo de la web IEEE Xplore publicado con el nombre **“La investigación e implementación de la VPN Gateway basada en SSL”**, por Chen Fei.

Nos comenta que la tecnología VPN es el uso del conocimiento de la criptografía en la red pública y abierta para establecer una red privada virtual. IPSec VPN y SSL VPN son dos tipos de tecnología y productos VPN que se utilizan actualmente y en la totalidad de casos. IPSec VPN funciona en la capa de red, SSL VPN funciona en la capa de sockets seguros. SSL VPN utiliza una serie de técnicas criptográficas, que incluyen cifrado simétrico, cifrado asimétrico, firmas digitales, certificados digitales y un algoritmo de resumen de mensajes. Este artículo analiza el principio de la tecnología VPN y el protocolo SSL. Propuse una solución de puerta de enlace VPN basada en el protocolo SSL. (Fei, 2013)

2.1.2. Base Teórica

2.1.2.1.Red Privada Virtual

Una VPN (Virtual Private Network). Es una manera de conectarse de forma íntegra, directa y segura a la red de su organización permitiendo a los usuarios remotos conexiones seguras desde cualquier lugar del mundo. El rol principal de la VPN para trabajo remoto es asegurar la comunicación entre el usuario y la red de LAN de la empresa o entidad.

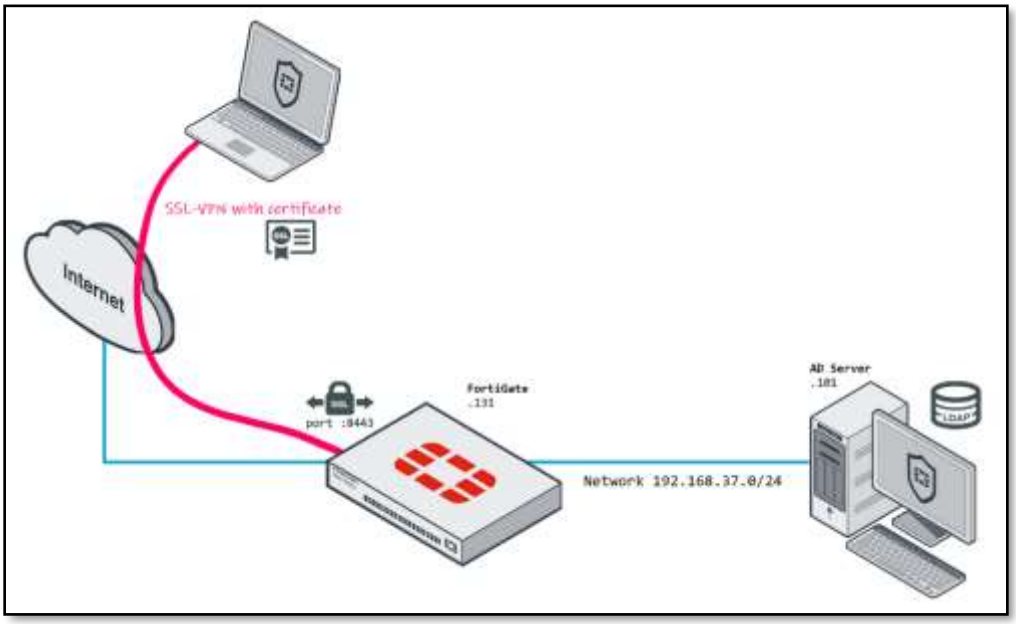


Figura 2. Acceso mediante una VPN.

Una VPN es una tecnología de red que permite una conexión segura a través de Internet conocida como túnel, a través de un método de encapsulación y encriptación de la data y sus paquetes a diferentes sitios remotos mediante el uso de tecnologías de transporte públicas en la nube. Incluso, posibilita que la computadora en la red pueda emitir o recepcionar datos como si se tratara de estar directamente en la red. (De la Cruz, 2019).

2.1.2.2.Ventajas de una VPN

Implementar una VPN cuenta con varios puntos provechosos:

- Integridad, punto en el que hace alusión a que un mensaje o dato no logre ser alterado.
- Confidencialidad, punto en que hace referencia a la autorización de los datos y el manejo prudente de su información.
- Encriptación, cumple la función de cifrar los datos que viajan a través de la VPN con el fin de no poder ser procesados por personas a las que no están destinadas.
- Reducción de costos y facilidad de uso.
- Simplifica la comunicación por medio de un aplicativo gratuito desde cualquier parte del mundo.

2.1.2.3.Requerimientos básicos de una VPN

Al implementar una solución VPN, es necesario facilitar el acceso auditado y supervisado a los recursos e información de la organización. La solución debe permitir que los clientes remotos se conecten a los recursos de la red interna. Adicionalmente, es vital garantizar la privacidad y la integridad de los datos en la forma que son expuestas a Internet. El mismo escenario es aplicado para el caso de datos confidenciales que cruzan una red interna de dicha entidad.

En consecuencia, una VPN como solución debe proveer requisitos basados en: compatibilidad, seguridad, disponibilidad e interoperabilidad. (Peña, 2016)

Compatibilidad

El protocolo de Internet (IP) debe ser compatible para que de esta manera una VPN pueda utilizar internet. Esta consideración se logra con la finalidad de asignar y usar grupos de direcciones IP. No obstante, gran cantidad de redes emplean direcciones IP privadas malgastando así la administración de direcciones. En la actualidad existen múltiples técnicas para hacer compatible la comunicación entre los segmentos privados e Internet, como la traducción de direcciones locales a internet NAT (Network Address Traslation) y el uso de túneles para su enmascaramiento y encapsulación.

Mediante esta técnica las direcciones de Internet convivirán con las redes IP privadas en el interior de una infraestructura de enrutadores de cualquier entidad. De esta forma, un cliente con una IP local logra ingresar al exterior por medio esta traducción de direcciones IP públicas sin necesidad de instalar previamente un software o agregar algún tipo de acción particular.

Seguridad

Se debe considerar y garantizar la protección frente al análisis de tráfico el cual podría ser interceptado mediante un sniffer capturando información y posteriormente hacer uso inadecuado de ella. Para esto la información viajará encriptada utilizando su propio método de cifrado de datos, de esta manera garantizamos que no se podrá extraer información valiosa por el mecanismo ofrecido en la configuración. El contenido no

debe ser alterado y tanto el emisor como el receptor deben transmitir de manera segura y ser protegido por un posible atacante.

Disponibilidad

Existen variables para que la disponibilidad sea impulsada y motivada a ser un requerimiento necesario, la facultad de mantenerse accesible en el sitio, en el momento y en el modo en que los usuarios que estén autorizados lo soliciten precisamente. Es primordial que tanto el software como el hardware se mantengan en funcionamiento de manera eficaz, en caso contrario, se pueden producir pérdidas descomunalmente económicas, daños materiales, y finalmente la desacreditación de la solución propuesta ante cualquier escenario.

Interoperabilidad

En redes y comunicaciones hablar de interoperabilidad hace una referencia directa que apunta a la capacidad de conectar usuarios y redes de forma que las variaciones en aplicaciones o servicios sean tolerables y no se perciban estas diferencias. Razón por la cual, previamente a adquirir una tecnología VPN, se debe tener presente como responsabilidad una forma de fortalecer una adecuada interoperabilidad la cual esta alojada como solución completa de acuerdo a los diferentes fabricantes existentes en el mercado competitivo. Siendo el caso en el que el supuesto fabricante no este apto de cumplir todas las necesidades, se procede a limitar y comparar con otras ofertas que, si cumplan estos requisitos y mejor aún si ofrecen un valor agregado, además de contar

con disponibilidad de laboratorios en los cuales la propuesta sea sometida a pruebas antes del despliegue y operación del proyecto para que sea viable.

2.1.2.4.Componentes de una VPN

Para un caso emulado de VPN punto a punto los datos son encapsulados o empaquetados mediante un encabezado que brinda la información de enrutamiento que permite a estos datos viajar por la red pública hasta llegar a su destino. Para el caso de una VPN privada, los datos son cifrados para garantizar la confidencialidad. En una red compartida o publica los paquetes interceptados no son descifrables mientras no se disponga de las claves de cifrado. Por consiguiente, el espacio de conexión donde los datos privados son encapsulados es distinguida como túnel mientras que parte de la conexión en que los datos privados son cifrados y encapsulados es denominado conexión VPN. (Gonzáles, 2006)

A continuación, se muestra la relación de componentes básicos que forman parte de una VPN:

- Servidor VPN
- Túnel
- Conexión VPN
- Red publica
- Cliente VPN

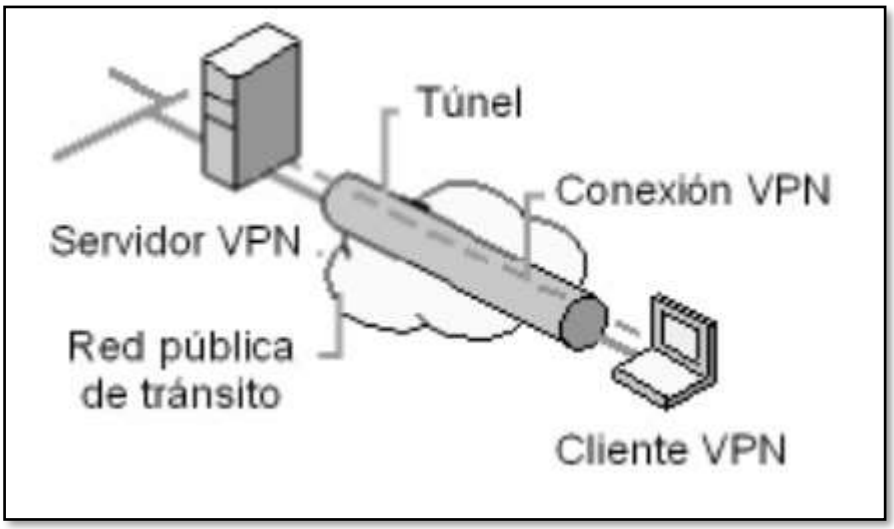


Figura 3. Componentes de una VPN

2.1.2.5.Categorías de una VPN

Las dos categorías principales de productos VPN para elegir son los dispositivos de hardware VPN dedicados y las VPN basadas en servidor, también denominadas VPN de hardware y software.

VPN de hardware

Una VPN de hardware ejecuta su red a través de un equipo dedicado que tiene su propio procesador y firewall. Este tipo de VPN es superior en dos áreas principales: seguridad y velocidad. El hecho de que la VPN de hardware solo maneja sus propias funciones, en lugar de ejecutarse sobre un dispositivo de propósito general, lo hace menos vulnerable a los ataques, mientras que su procesador dedicado evita que se consuman

los ciclos de CPU de sus servidores. En el lado negativo, las VPN de hardware pueden ser costosas, y cuanto más necesite escalar, más se puede obtener con la propuesta.

Figura 4. Equipo de seguridad perimetral FortiGate-100E

VPN de software

Un software VPN es una aplicación que se ejecuta en un servidor. Las mayores ventajas de las VPN de software son la asequibilidad y la escalabilidad. Una VPN de software implicará una inversión inicial más baja que una VPN de hardware, y la ampliación es tan simple como actualizar los componentes del servidor de vez en cuando. En el lado negativo, su VPN será tan segura como el hardware en el que se está ejecutando, y la compartición del procesador / memoria probablemente hará que se atrase con respecto a las velocidades de VPN de hardware.

Figura 5. Las mejores VPN de software libre usadas en 2019

Fuente: https://medium.com/@ProdLandHQ/the-11-best-vpn-services-of-2019-free-vpn-software-and-tools-6aad22644d3d

2.1.2.6.VPN Hardware vs VPN Software

Tabla 1. Comparación entre VPN de hardware y software

	VPN por Hardware	VPN por Software
Costo	En su generalidad las VPN por hardware suelen ser mas costosas.	Las VPN por software no son costosas y en especial si es de software libre.
Escalabilidad	Depende del modelo y al costo asociado a la actualización de un modelo mas grande. Limitada por la licencia.	La escalabilidad se basa en la actualización generalmente se traduce en reemplazar un procesador integrado o agregar memoria al sistema.
Seguridad	Son más seguras ya que la única función del harware es la administración de conexiones VPN.	Se ven obligadas a compartir un servidor con otras aplicaciones y sistemas operativos, lo que los hace mas propensos a los ataques y menos seguros.
Mantenimiento	Estan sujetos a contratos de soporte de mantenimiento que le dan derecho a actualizaciones y soporte de software.	Algunas VPN de software de código abierto, estan disponibles de forma gratuita y no tienen costo de mantenimiento elevados.
Rendimiento	Ofrecen mejor rendimiento, por lo que se dedica a una sola tarea, ofrecen equilibrio de carga.	Las soluciones VPN basadas en servidor a menudo están restringidas porque coexisten con otras aplicaciones, lo que restrige su rendimiento.

2.1.2.7.Tipos de VPN

Hasta el momento contamos con dos tipos de VPN, estos son los siguientes:

VPN de acceso Remoto

La VPN de acceso remoto concede a los usuarios acceder a los datos y recursos de la organización en el momento que lo requieran. Basta tener instalado un cliente VPN en el dispositivo y el usuario será capaz de conectarse a la red interna de la organización sin distinguir zona geográfica donde se ubique. Estos equipos clientes son denominados como puntos finales los cuales pueden ser teléfonos inteligentes, tablets, computadoras, etc. El avance tecnológico para una VPN incluso ha permitido el análisis de seguridad

en los dispositivos finales con el fin de garantizar que cumplan los requisitos de seguridad antes de la conexión. (Gonzáles, 2006)

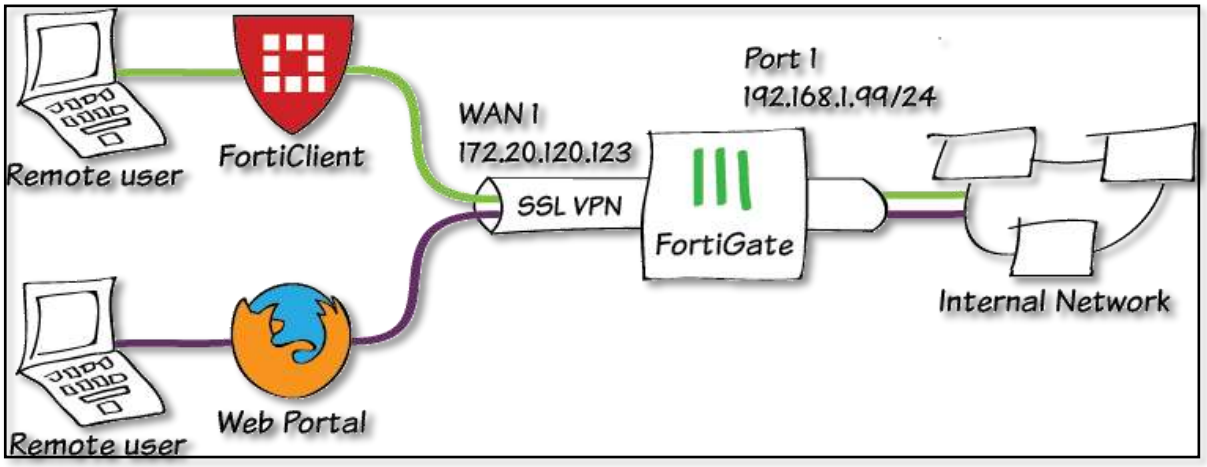


Figura 6. Representación de acceso VPN SSL

VPN Site to Site

La VPN site-to-site comunica o interlaza una oficina con sus demás sucursales mediante Internet. Este tipo de VPN es utilizado cuando por temas de distancia no amerita poseer conexiones directas entre redes u oficinas remotas. La solución o equipo es designado puntualmente para fijar y mantener activa esta conexión. Tiene que verse y tener claro que una VPN sitio a sitio es como una comunicación de una red con otra red.

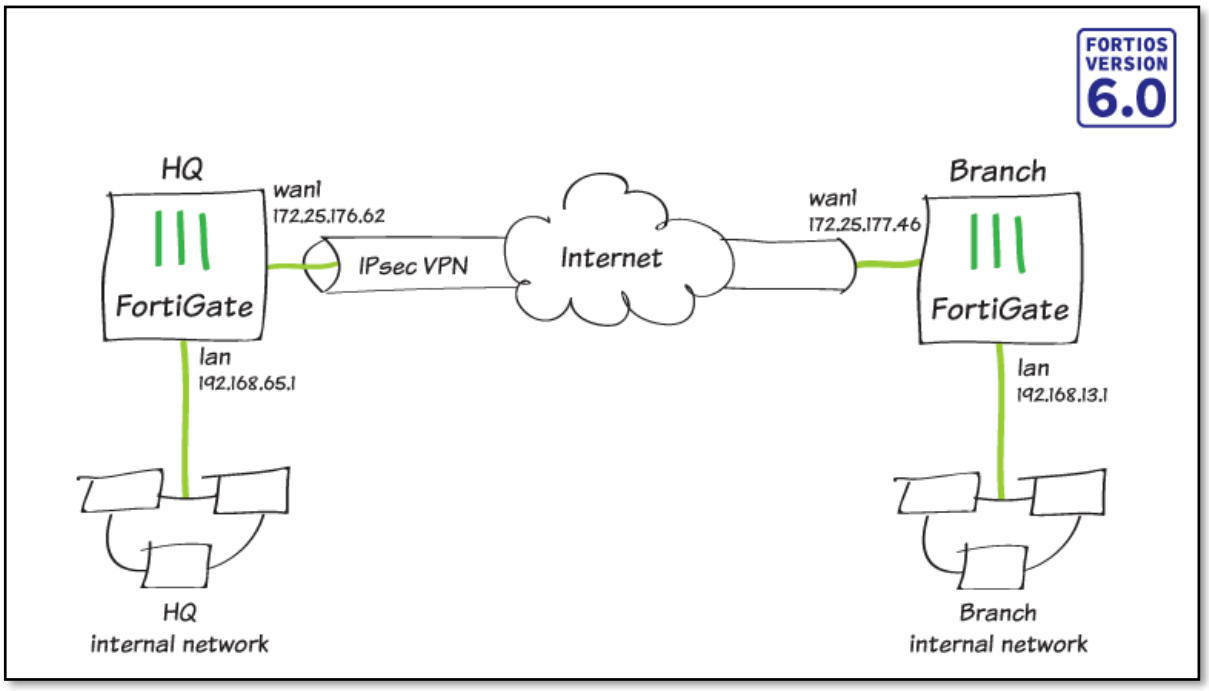


Figura 7. Representación de una conexión VPN Site to Site

2.1.2.8.Protocolos de conexión VPN

Protocolo IPSec

IPsec como protocolo seguro de Internet ofrecen algoritmos de seguridad más robustos y métodos de encriptación más complejas y la autenticación más completa. Este protocolo IPSec tiene dos modos o formas de encriptación: túnel y transporte. (Perdomo, 2018)

Modo de transporte

En el escenario de IPsec la carga útil efectiva del paquete se cifra y autentica, mientras que la información del encabezado es integra.

Modo de túnel

El paquete es cifrado, luego de ser cifrado este mismo se encapsula para crear un paquete IP actual que posee información diferente en su encabezado.

Además, todos los componentes de cada punto deben hacer uso de una clave común o certificarla y deben contar con la configuración muy parecida a las políticas de seguridad.

IPSec viene a ser un protocolo comúnmente usado para trasladar datos de modo seguro en la capa de red. Para ser más concretos, este protocolo mejora la seguridad del protocolo IP garantizando solo así la privacidad, probidad y legitimidad de los datos que son enviados.

Protocolo PPTP/MPPE:

El PPTP (Point-to-Point Tunneling Protocol) originada por la compañía PPTP la cual tiene como aliados a 3COM, Microsoft, US Robotics, etc. Este sujeta el multiprotocolo VPN conformada por 40 bits y un cifrado de 128 bits en colaboración de Microsoft es denominado Microsoft Point-to-Point Encryption (MPPE). PPTP fue creado para admitir a los clientes la conexión a un servidor RAS mediante algún punto de Internet

obteniendo así la misma encriptación, autenticación y similares accesos de una red local como discado directo al servidor.

Protocolo L2TP:

Este protocolo por sí mismo no otorga algún servicio de confidencialidad o encriptación de manera automática, es usado como protocolo de túnel que soporta la VPN o como ámbito de prestación de concesión por un ISP.

Integrada del resultado de compañías integrantes como PPTP, Cisco y la IEFT, L2TP es convocado sobre IPsec, brindando seguridad en la tunelización del protocolo IPsec y que es utilizado en los sistemas operativos Windows Server para el acceso VPN hacia estos sistemas, cabe mencionar que Windows Server provee IPsec y L2TP originario a un cliente.

Protocolo SSL

El protocolo SSL que tiene como traducción (Capa de Conexiones Seguras), viene a ser un protocolo que maneja y aplica certificados digitales para constituir o fijar una comunicación segura mediante Internet.

Dicho protocolo SSL está diseñado para admitir que las aplicaciones logren transmitir ida y vuelta información de forma segura. Incluso las mismas aplicaciones que hacen uso del protocolo SSL utilizan su propio clave de cifrado para emitir y recibir datos con otras aplicaciones, cifrando y descifrando los datos de manera bidireccional.

Protocolo TLS

El protocolo TLS tiene multitud de aplicaciones en uso en la actualidad. La mayoría de ellas está plasmada en programas con versiones seguras. TLS es ejecutado en protocolos basados en aplicación como lo es la capa HTTP, mediante SSL/TLS se convertiría en HTTPS ofreciendo así seguridad para enlaces que utilizan WWW o para tráfico electrónico como aplicación, comprobando la autenticidad de extremos mediante certificados de clave pública. SSH utiliza también SSL como TLS, SMTP también puede operar de manera segura sobre SSL y TLS, POP3 e IMAP4 sobre SSL/TLS.

2.1.2.9.Firewall

Un firewall (cortafuegos), es un sistema de seguridad diseñado específicamente para bloquear el acceso no autorizado a comunicaciones peligrosas. Pueden ser de software o hardware, estos permiten que todos los mensajes que entran o salen de la intranet pasan a través del cortafuegos, el cual examina cada mensaje y bloquea los que no cumplen los criterios o políticas ya establecidas en el mismo.

Su ubicación usualmente es en un punto de conexión de la red LAN de la organización con la red WAN externa que habitualmente es Internet; de esta forma la red interna es protegida de intentos no autorizados, ataques, vulnerabilidades que puedan existir en los sistemas de la red interna. (Conza, 2009)

Principales fabricantes de Firewall

Fortinet: Empresa privada norteamericana, dedicada esencialmente a esquematizar y fabricar elementos y mecanismos de seguridad para la variedad exigente de redes (Firewall, UTM, etc.)

En la actualidad es la marca de posición y la más innovadora en sistemas de seguridad UTM, superando auténticamente a marcas como Cisco o CheckPoint en la contienda competencial del mercado.

Las aplicaciones y plataformas de Fortinet integran sofisticadas particularidades de red, capacidad de alta disponibilidad, capacidades virtuales de dominio, protección rentable, comprensiva contra las amenazas de la red e internet.

Figura 8. Imagen de la marca Fortinet

Cisco: Cisco Systems liderando en el mundo de redes e Internet transformando muchos sectores y empresas como parte integral de sus soluciones afianzando y fidelizando a sus clientes en relaciones duraderas, colaborando conjuntamente con ellas para el impulso de nuevas necesidades identificadas con visión de éxito. Su diversidad también mantiene su lucha en el mercado de las tecnologías.

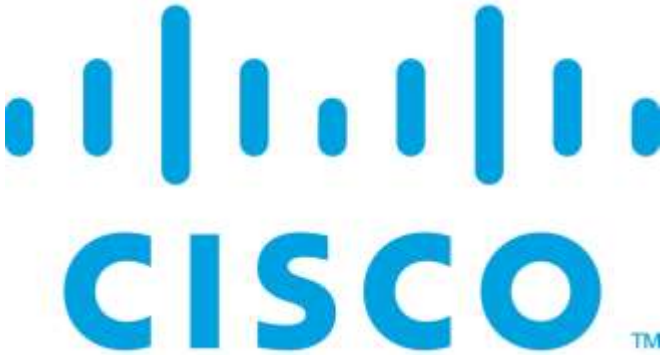


Figura 9. Imagen de la marca Cisco

SonicWall: Prestigioso fabricante constituida desde 1991 el cual brinda sistemas de seguridad como SSL, Aceleradores, Cortafuegos, VPN, entre otros) tiene un portafolio de productos de excepcional calidad y de gran ventaja económica facilitando dese las Pymes hasta grandes empresas que brindan servicios, a nivel mundial sus productos son incorporados por múltiples empresas.

Figura 10. Imagen de la marca SonicWall

Check Point: Checkpoint Software Technologies LTD, fundada en 1993, sus soluciones están basadas exclusivamente en seguridad lógica únicamente, con cobertura desde usuarios pequeños hasta grandes proveedores de Internet.

Figura 11. Imagen de la marca Check Point

Palo Alto: Se trata de una compañía de ciberseguridad residente en Santa Clara, California. Su gama de productos bandera se comprende de firewalls avanzados y ofertas basadas en la nube que extienden esos firewalls para cubrir otros aspectos de la seguridad.

Figura 12. Imagen de la marca Palo Alto

2.1.2.10. FortiGate UTM

La misión de Fortinet es ofrecer la red más innovadora y de mayor rendimiento estructura de seguridad para asegurar y simplificar su infraestructura de TI. Es un líder mundial de proveedor de dispositivos de seguridad de red para operadores, centros de datos, empresas y oficinas distribuidas. (Acacio, 2020)

FortiGate es un equipo desarrollado por Fortinet como cortafuegos de hardware, con múltiples funcionalidades de detección de virus, amenazas y otros ataques como contenido, actuando sin afectar el mecanismo de tiempo real de una red, su rendimiento y capacidad de filtro de contenido, antivirus, protección contra intrusos, control de tráfico y balanceo permite formar un fornido esquema de red protegida. (Orosco, 2018)

Figura 13. Representación UTM de FortiGate Gestión unificada de amenazas

2.1.2.11. FortiAnalyzer

FortiAnalyzer es la herramienta de análisis de seguridad NOC-SOC construida con perspectiva de operaciones. Con vistas orientadas a la acción y capacidades de desglose

profundo, FortiAnalyzer no solo brinda a las organizaciones información crítica sobre las amenazas, sino que también analiza con precisión el riesgo en toda la superficie de ataque, señalando dónde se requiere una respuesta inmediata.

Una arquitectura de seguridad integrada con capacidades de administración de registros y seguridad basada en el análisis puede solucionar esta falta de visibilidad. Como parte del Security Fabric de Fortinet, FortiAnalyzer apoya casos de uso basados en análisis para proporcionar una mejor detección contra violaciones. (Fortinet L. , 2021)

Figura 14. Equipo físico FortizAnalyzer-200D (FAZ)

El Appliance FortiAnalyzer se representa de la siguiente manera en una red:

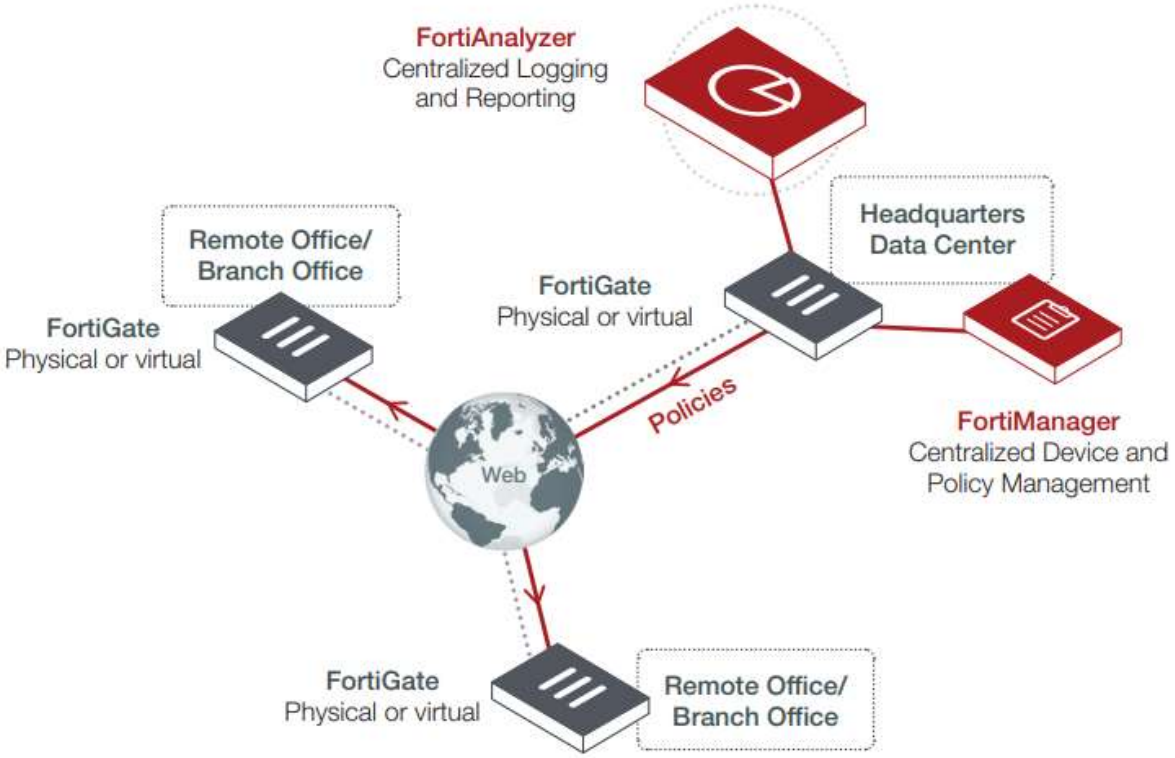


Figura 15. Representación gráfica del FortiAnalyzer instalado en una red

Figura 16. Portafolio de productos marca Fortinet

2.1.2.12. Autenticación Multifactor

La comunicación y las tecnologías de la información poseen un gran valor en la vida cotidiana, ya que las ellas se han vuelto un instrumento de uso habitual. Debido al número de patrones de usos, existe una progresiva exigencia de garantizar su adecuado funcionamiento y de la misma manera su adecuada operación.

La autenticación es un componente fundamental de un prototipo de seguridad. Es de vital importancia la diferencia entre autenticar y autorizar, que es otra pieza fundamental como propósito de seguridad. Para comprobar la identidad el usuario aplica autenticación. Por otra parte, el usuario comprueba y confirma un permiso correcto con derechos de ingreso a determinado lugar o cierto recurso, esto es denominado autorización.

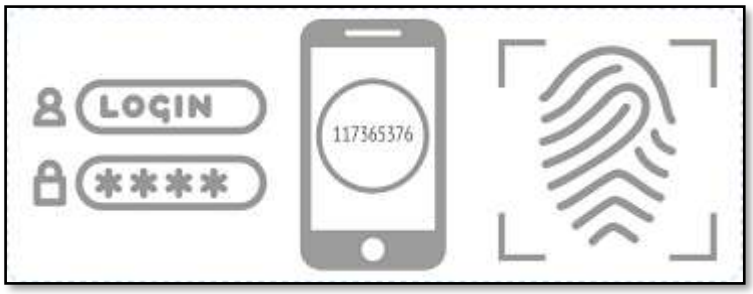


Figura 17. Representación de una Autenticación Multifactor

Actualmente se conservan tres escalas como nivel de autenticación: Claves de información, claves físicas y claves biométricas, las cuales se basan en tres formas que el usuario puede comprobar respectivamente a partir de:

Algo que la persona sabe

En este apartado el usuario provee información que solo el conoce, puede ser una clave, PIN, enunciado de contraseña o preguntas y juego de respuestas.

Algo que la persona posee

Aquí el usuario otorga un ítem que posee, como un token o una contraseña de un solo uso.

Algo que la persona es

El usuario confía en un rastro o característica única de su persona incluyendo huellas dactilares, inspección de voz, inspección facial, examinación de retina, escaneos y reconocimientos que permita responder a un servidor ese acceso único detrás de la escena.

Sin embargo, para lograr una autenticación de múltiple factor sea posible esta deberá incluir dos o más métodos mínimos como autenticación con la finalidad de reforzar una consistente autenticación. (García, 2016)

2.1.2.13. FortiToken Mobile

FortiToken Mobile (FTM) es una aplicación generadora de contraseña única (OTP) basada en eventos y en el tiempo compatible con OATH para el teléfono móvil inteligente. Es el componente cliente de la solución elevadamente segura, fácil de usar y administrar, y extremadamente productiva y beneficiosa de Fortinet para complacer las fuertes exigencias y requisitos de autenticación. Puede implementar tokens FTM

utilizando FortiOS, FortiAuthenticator o FortiToken Cloud (2FA-as-a-Service) como servidor de validación back-end para tokens FTM. Hay disponibles notificaciones automáticas para aprobar o denegar intentos de inicio de sesión. FTM también admite tokens de terceros para los sitios web más populares. (Fortinet I. , 2021)

Figura 18. FortiToken Mobile disponible en Play Store

Las claves y contraseñas no descartan la posibilidad de visitantes no deseados en la red. Es por eso que la autenticación con solo una contraseña abre paso a brechas de seguridad, expansión y contaminación de variantes de malware y el incumplimiento de políticas quizá ya establecidas. Con un doble factor de autenticación podrás combinar una contraseña adyacente a un token de seguridad y para proporcionar mayor seguridad un servidor auntenticador. Los usuarios autorizados pueden ingresar a los recursos de la empresa de modo seguro combinando diversos dispositivos, que involucran computadoras hasta teléfonos inteligentes. FortiToken Mobile actúa como un token físico pero que está representado como una aplicación para Android o iOS utilizando un dispositivo móvil para la interacción conjunta con el usuario.

2.1.2.14. Metodología PPDIOO de Cisco

La metodología PPDIOO tiene como origen lineamientos planteados en el ciclo de vida PPDIOO que utiliza Cisco en administración de red. El recorrido de este ciclo de vida permite cumplir objetivos trazados, entre ellos la disminución del costo total de la administración y aumento de disponibilidad de la red, agilizando la estructura de red. Este ciclo de vida es un bucle sin fin ya que en la fase de optimización siempre se van a identificar actividades y cambios hasta en la misma infraestructura existente, la cual sería nuevamente analizada partiendo del primer paso que es preparación. (Erazo, 2016)

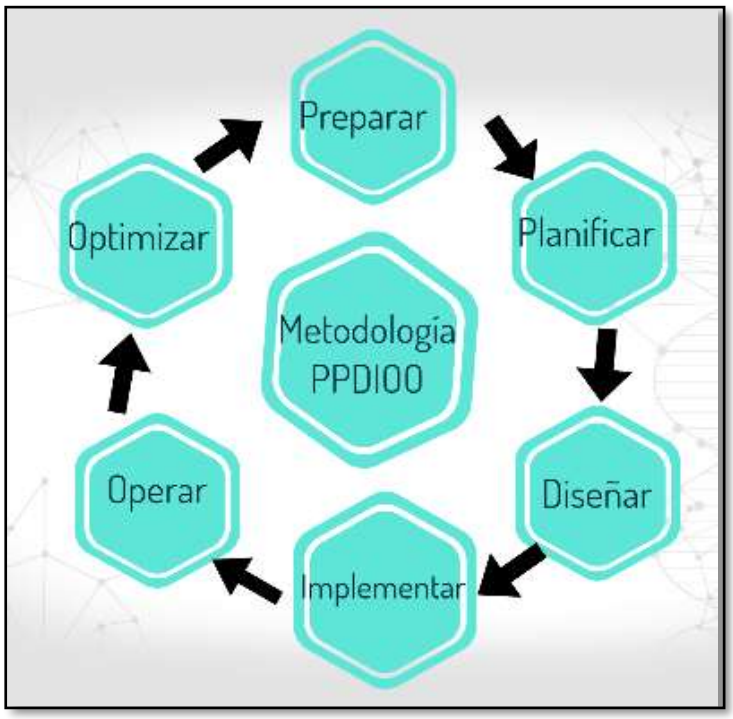


Figura 19. Representación de la metodología PPDIOO

Fases del ciclo de vida PPDIOO

PPDIOO abarca en cada primera letra en ingles un significado compuesto por:

- **P (Prepare) Fase de Preparación** compromete factor presupuestal, táctica de red.
- **P (Plane) Fase de Planeación** compromete determinación de la red, análisis de desperfectos.
- **D (Design) Fase de Diseño** compromete un diseño como solución (servicios, paquetes).
- **I (Implement) Fase de Implementación** implica la puesta en marcha del producto.
- **O (Operate) Fase Operativa** implica un mantenimiento para dicha solución.
- **O (Optimize) Fase de Optimización** compromete la administración constante de la red.

Fase de Preparación

Fase en la cual se anticipa una visión general, requisitos y tecnologías indispensables para edificar y mantener una ventaja competitiva. En general esta etapa depende de un argumento financiero como caso de negocio para fijar una estrategia de red que resuelva problemas o deficiencias determinadas como requerimientos del cliente o usuario final.

Fase de Planeación

La fase en general se identifica por aplicar una revisión de la red actual basado en el estudio de desperfectos versus las buenas prácticas, que durante el desenlace del proyecto se aplicaran medios y objetivos. Esta etapa considera la validación de recursos, sus poderosos riesgos involucrados que incluyen software y hardware, de la misma forma si existe recursos humanos libres. Una buena determinación en la red requiere estratégicamente herramientas de análisis del comportamiento actual de la red y manifiesta alternativas a aplicar, la recolección de información en esta etapa es fundamental para la elección de materiales requeridos.

Fase de Diseño

La fase en general empieza con un diseño de red según la recolección de datos resultado de la fase anterior. La información más detallada y especifica será parte del plan de proyecto como actualización, esta será de gran ayuda para la implementación. El diseño correcto se comprende de objetivos alineados con solicitudes técnicas y facultando los cambios, lo que se va descartar o agregar a la red con visibilidad adquirida y existente brindando un mejor servicio.

Fase de Implementación

A partir de esta fase se lleva a cabo la instalación y configuración de los equipos. En términos de proyecto el plan de trabajo deber ser cumplido, previamente conversado y

aceptado por el equipo de trabajo. El tiempo evaluado y documentado debe proveer un plan de contingencia, así como un rollback aplicado en caso de fallo general. Su principal objetivo es implementar la solución sin implicar la red y su disponibilidad definiendo ventanas de tiempo para lograrlo. Es esencial ejecutar una prueba piloto en un ambiente de preproducción para el efecto de permitir simular un entorno real.

Fase de Operación

Esta etapa conserva un día a día en la red incluyendo su administración y monitoreo de sus elementos, gestión del desempeño y la subsanación identificada de errores, temas que serán identificados, documentados y corregidos. Esta fase tiene como objetivo principal mantener un estado de salud optimo y de brindar un mejor servicio, reduciendo interrupciones y brindando mayor disponibilidad, fiabilidad y seguridad. Para realizar un reporte y monitoreo correcto podemos utilizar herramientas que nos ayuden a proveer acciones preventivas y correctivas inmediatas sin la percepción del usuario final.

Fase de Optimización

Esta fase se tiene en cuenta la acción proactiva, identificando y mejorando la red continuamente. Esta fase como objetivo principal tiene reforzar la carga de la red sin generar interrupciones a la ejecución y adecuándose a los cambios y requisitos de actualización tecnológica y del mundo.

2.2. Marco conceptual

Active Directory: Condición usada por Microsoft para mencionar a su implementación de servicio de directorio en una red conformada de grupos y usuarios.

Acceso Remoto: La capacidad de controlar un equipo desde otra ubicación, tipo de conexión que normalmente es usada en cualquier red.

Ancho de banda: Secuencia de frecuencias medibles otorgadas por un proveedor de servicios de internet, se miden en Hertz.

Autenticación: Método que determina la autorización y permiso del usuario para el acceso a un recurso o para ejecutar una operación.

Firewall: Es un dispositivo de funciones múltiples de acuerdo al fabricante o marca el cual funciona como cortafuegos entre segmentos de red, permitiendo o denegando conexiones de una red a otra.

Gateway: Es una "puerta de enlace" entre dos redes distintas, entre una red local y una extensa WAN (equipo para interconectar redes).

ISP: Es una entidad, la cual brinda acceso a Internet a personas físicas y/o jurídicas, les ofrece un portafolio amplio de servicios como páginas web, consultoría de webs e Intranets.

Internet: Red global de equipos cuyas comunicaciones se realizan mediante un protocolo común, TCP/IP.

LDAP: Base de datos que guarda y administra directorios con información de usuarios de la red a través de protocolos TCP/IP ya estandarizados.

Protocolo TCP/IP: Sus siglas significan "Protocolo de control de transmisión/Protocolo de Internet. Un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, etc.

SSL: Protocolo que suministra privacidad y autenticación de los datos como medio criptográfico ante extremos como habitualmente lo es Internet.

UDP: Es un protocolo de datagramas de usuario, el cual emite a través de la red sin haber dispuesto anticipadamente una conexión.

VPN: Red privada virtual que permite crear un túnel de conexión segura para el acceso de usuarios autorizados que harán uso de los recursos de la organización como si estuviesen directamente en la red.

2.3.Marco metodológico

Para este informe de suficiencia profesional se adaptará la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar) en un singular Marco Metodológico, esto facultará el progreso completo de diseño e implementación en la red informática de la entidad, ya que el enfoque principal de esta metodología es plasmar las actividades y necesidades en base a la propuesta de implementar una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte, permitiendo brindar seguridad a nuestros usuarios y a la información comprometida que será parte de esta conexión.

El Marco Metodológico propuesto constará de cuatro etapas las cuales serán:

2.3.1. Etapa de Organización

Como primera etapa del Marco Metodológico, en esta se llevará a cabo las siguientes actividades:

- Componentes de la Red HV - Servidores Físicos
- Aplicaciones de la Red HV - Servidores Virtuales
- Diagrama de Red Actual HV
- Selección de la tecnología para la implementación – Datasheet del Producto

2.3.2. Etapa de Análisis y Diseño

Como segunda etapa se analizará los recursos humanos y físicos que participaran para integrar la solución futura y seguidamente el diseño de la propuesta a implementar, se llevara adelante las siguientes actividades:

- Análisis de Requerimientos (TDR y ETT)
- Requerimiento del usuario final
- Requerimiento para las aplicaciones y sistemas del HV

- Requerimiento de infraestructura (Análisis Técnico)
- Asignación de personal como recurso de implementación
- Plan de trabajo (Diagrama de Gantt)
- Modelo de Negocio
- Direccionamiento IP propuesto
- Diagrama de Red Propuesto (VPN-SLL + Doble Factor de Autenticación + FAZ)

2.3.3. Etapa de Desarrollo e Implementación:

- Configuración del FortiGate-100E
- Configuración e integración del protocolo LDAP en el Firewall
- Agregando los grupos del dominio en el Firewall
- Configuración de la VPN-SSL para el acceso remoto
- Creación de políticas de acceso para los usuarios VPN
- Asignación de FortiToken virtual a usuarios VPN como Doble Factor de Autenticación
- Prueba piloto de conexión VPN-SSL con método de Doble Factor de Autenticación

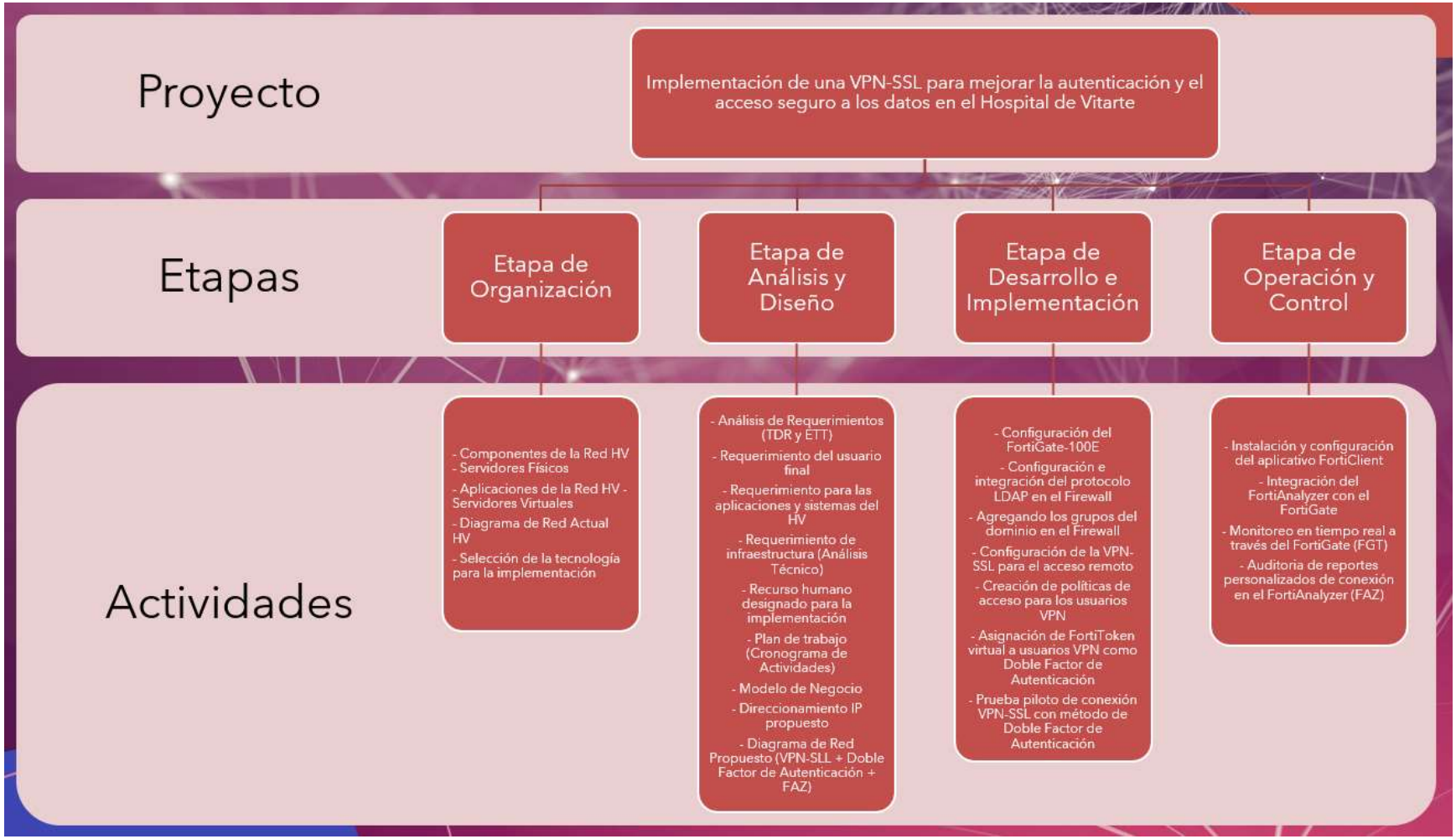
2.3.4. Etapa de Operación y Control

En esta etapa se llevará a cabo un conjunto de actividades de gestión que permitirá verificar que el despliegue de la implementación sea controlable y auditable lo mejor posible.

- Instalación y configuración del aplicativo FortiClient
- Integración del FortiAnalyzer con el FortiGate
- Monitoreo en tiempo real a través del FortiGate (FGT)
- Auditoria de reportes personalizados de conexión en el FortiAnalyzer (FAZ)

Estructura de desglose de trabajo (EDT)

Tabla 2. EDT del Proyecto



CAPITULO 3

3. DESARROLLO DE LA SOLUCION

3.1.ETAPA DE ORGANIZACIÓN

Componentes de la Red HV – Servidores Físicos

Como parte de esta etapa recolectaremos información con respecto a los servidores físicos con los que cuenta el Data Center del Hospital de Vitarte.

MARCA	MODELO	HOSTNAME	PROCESADOR	N° Cores
DELL	**R730**	**HYPERV-04**	Intel Xeon CPU E5-2687W v4 - 3.00GHz (2 procesadores)	24
MARCA	**MODELO**	**HOSTNAME**	**PROCESADOR**	**N° Cores**
IBM	**X3650 M4**	**HYPERV-03**	Intel Xeon CPU E5-2630 v2 - 2.60GHz (2 procesadores)	12
MARCA	**MODELO**	**HOSTNAME**	**PROCESADOR**	**N° Cores**
IBM	**X3650 M4**	**HYPERV-02**	Intel Xeon CPU E5-2680 v2 - 2.70GHz (1 procesador)	8

Figura 20. Servidores Físicos del Hospital de Vitarte

Aplicaciones de la Red HV – Servidores Virtuales

Tabla 3. Aplicaciones y sistemas en Servidores Virtuales

HYPERV-04 / DELL R730						
HOSTNAME	**IP**	**DESCRIPCION**	**CORES**	**MEMORIA RAM**	**DISCOS DUROS**	**Sistema Operativo**
DEMETER	172.16.1.35	ACTIVE DIRECTORY 2: HOSPITAL	8 Procesadores virtuales	8 GB	DISK01: 100 GB	Windows Server 2012 R2
HERA	172.16.1.5	AD01 PRIMARIO: HVITARTE	8 Procesadores virtuales	8 GB	DISK01: 100 GB DISK02: 50 GB	Windows Server 2012 R2
IRIS	172.16.1.21	IIS: SERVIDOR WEB / FTP	8 Procesadores virtuales	8 GB	DISK01: 100 GB DISK02: 50 GB	Windows Server 2012 R2
OSAKA	172.16.1.6	AD02 SECUNDARIO: HVITARTE	1 Procesadores virtuales	8 GB	DISK01: 200 GB	Windows Server 2012 R2
SEMELE	172.16.1.14	APLICATIVO SIAF	8 Procesadores virtuales	8 GB	DISK01: 100 GB DISK02: 50 GB	Windows Server 2012 R2
SENDAI	172.16.1.22	APP LLAMADA DE PACIENTES	1 Procesadores virtuales	8 GB	DISK01: 200 GB DISK02: 100 GB	Windows Server 2016
ARES	172.16.1.17	APP SIGPER	12 Procesadores virtuales	12 GB	DISK01: 100 GB DISK02: 50 GB DISK03: 50 GB	Windows Server 2012 R2
FARM01	172.16.1.10	W10 MULTISESION RDP	4 Procesadores virtuales	12 GB	DISK01: 200 GB	Windows 10 Enterprise
ARTEMISA	172.16.1.12	APLICATIVO SIGA	16 Procesadores virtuales	16 GB	DISK01: 100 GB DISK02: 50 GB DISK03: 25 GB DISK04: 50 GB	Windows Server 2012 R2
HESTIA	172.16.1.18	BASE DE DATOS: GESTION HOSPITALARIA	16 Procesadores virtuales	24 GB	DISK01: 100 GB DISK02: 150 GB DISK03: 150 GB	Windows Server 2012 R2

Diagrama de Red Actual HV

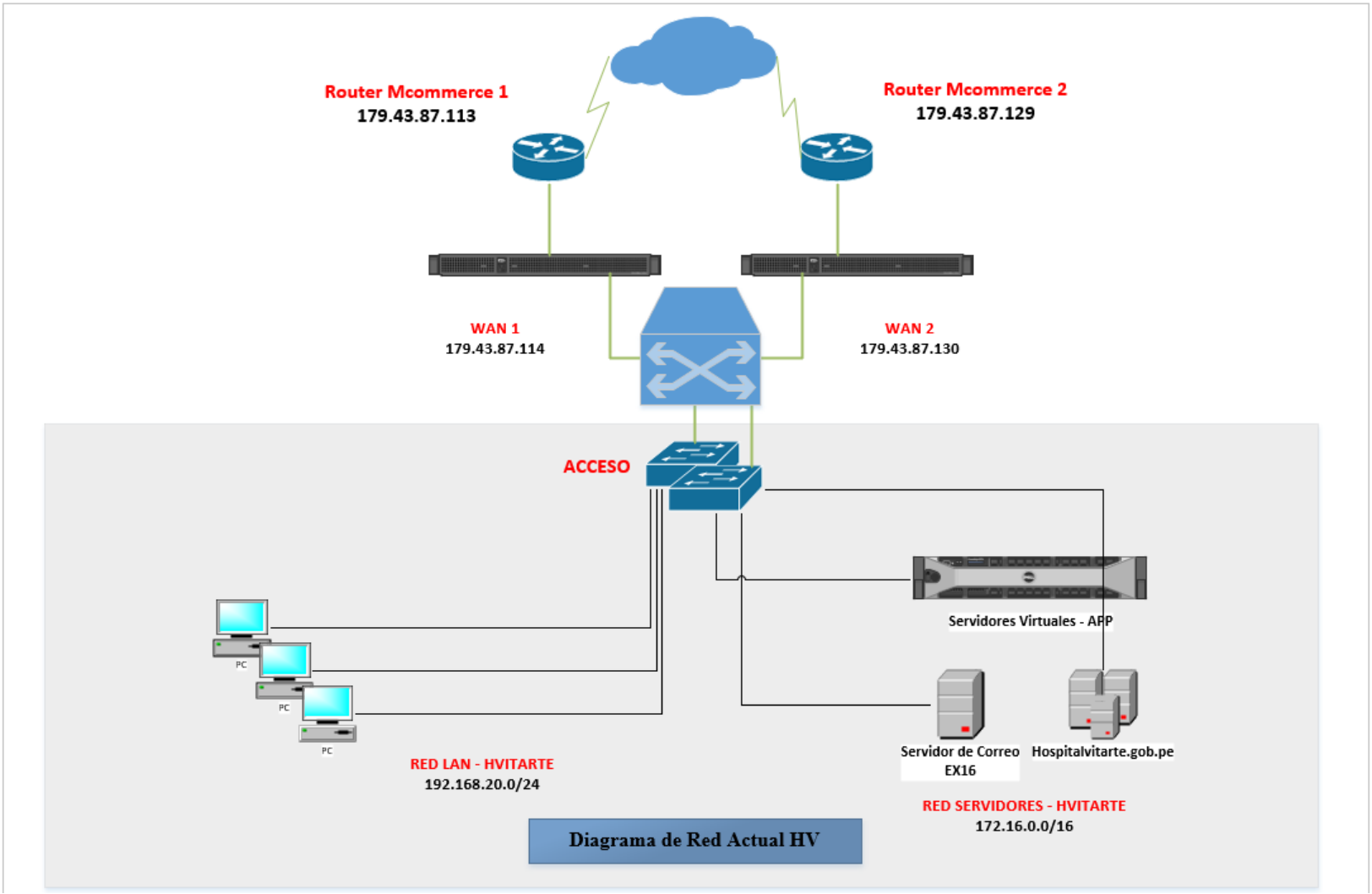


Figura 21. Diagrama de la Red Actual HV

Selección de la tecnología para la implementación

La tecnología para la implementación estará basada en la solución de marca Fortinet, y para poder lograr implementar una VPN-SSL vamos a adquirir el Firewall FortiGate-100E para el Hospital de Vitarte como dimensión. En el cual se integrará el protocolo LDAP para definir y declarar los grupos del dominio alojados en el servidor Active Directory de la institución.

Firewall FortiGate-100E – Datasheet (ANEXO 01)

Figura 22. Parte frontal del FortiGate-100E

Hardware

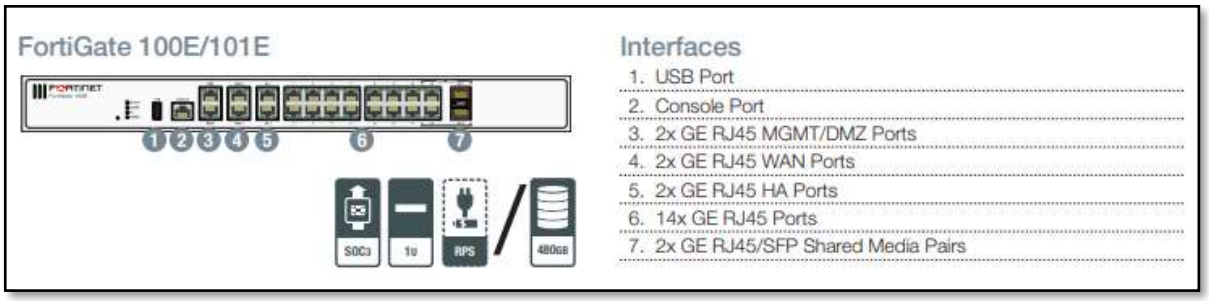


Figura 23. Interfaces del FortiGate-100E

Especificaciones Técnicas del producto

System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	7.4 / 7.4 / 4.4 Gbps
Firewall Latency (64 byte UDP packets)	3 µs
Firewall Throughput (Packets Per Second)	6.6 Mpps
Concurrent Sessions (TCP)	2 Million
New Sessions/Second (TCP)	30,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) [1]	4 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	250 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	130 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	130
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	125,000
Application Control Throughput (HTTP 64K) [2]	1 Gbps
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	32
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32
Maximum Number of FortiTokens	5,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

Figura 24. Especificaciones y rendimiento del FortiGate-100E

FortiToken Mobile – Datasheet (ANEXO 02)

FORTINET

DATA SHEET

FortiToken™ One-Time Password Token

Mobile (FTM) One-Time Password (OTP) Application with Push Notification
Hardware Token Time-Based OTP Form-Factors: FTK-200, FTK-200CD and FTK-220

Overview

Fortinet's FortiToken Mobile (FTM) and hardware OTP Tokens (FTK-200, FTK-200CD and FTK-220) are fully integrated with FortiClient, protected by FortiGuard and leverage direct management and use within the FortiGate and FortiAuthenticator security platforms. Secure your network with Fortinet's easy-to-manage, easy-to-use Two-Factor Authentication solutions.

PRODUCT OFFERINGS

FortiToken Mobile

FortiToken Mobile is an OATH compliant OTP generator application for the mobile device supporting both time-based (TOTP) and event-based (HOTP) tokens.

Figura 25. Datasheet del producto FortiToken Mobile

Especificaciones Técnicas

	FORTITOKEN MOBILE
Onboard Security Algorithm	OATH time and event based OTP generator
OTP Spec	RFC 6238, RFC 4226
Supported Platforms	iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows Phone 8/8.1, Windows 10 and Windows Universal Platform
Over-the-Air Token Activation	WiFi-only devices supported
One-Tap Approval	Login details pushed to phone
PIN/Fingerprint/Facial Security	✓
Serial Number Display	✓
Token and App Management	✓
Self-Erase Brute-Force Protection	✓

Figura 26. Especificaciones técnicas del FortiToken

Licencia de Software – FortiToken Mobile

Product	SKU	Description
FortiToken Software License Key	FTM-ELIC-5	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5 users. Electronic licence certificate.
	FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic licence certificate.
	FTM-ELIC-20	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 20 users. Electronic licence certificate.
	FTM-ELIC-50	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic licence certificate.
	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic licence certificate.
	FTM-ELIC-200	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic licence certificate.
	FTM-ELIC-500	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 500 users. Electronic licence certificate.
	FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 1000 users. Electronic licence certificate.
	FTM-ELIC-2000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic licence certificate.
	FTM-ELIC-5000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic licence certificate.
	FTM-ELIC-10000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic licence certificate.

Figura 27. Licencia para FortiToken según cantidad de dispositivos

3.2.ETAPA DE ANALISIS Y DISEÑO

Análisis de Requerimientos

Esta segunda etapa identificaremos los recursos existentes de la red del Hospital de vitarte, las actividades que se llevaran a cabo como diseño de la propuesta a implementar.

Términos de Referencia (TDR) para la contratación de servicios – Telefonía fija e Internet (ANEXO 03)

PERÚ Ministerio de Salud Hospital Vitarte	Directiva Administrativa "Que regula los procedimientos para la contratación de bienes y servicios cuyos montos sean iguales e inferiores a ocho (08) unidades impositivas tributarias (UIT)".	FECHA JUNIO 2019

TERMINOS DE REFERENCIA (TDR) PARA LA CONTRATACION DE SERVICIOS

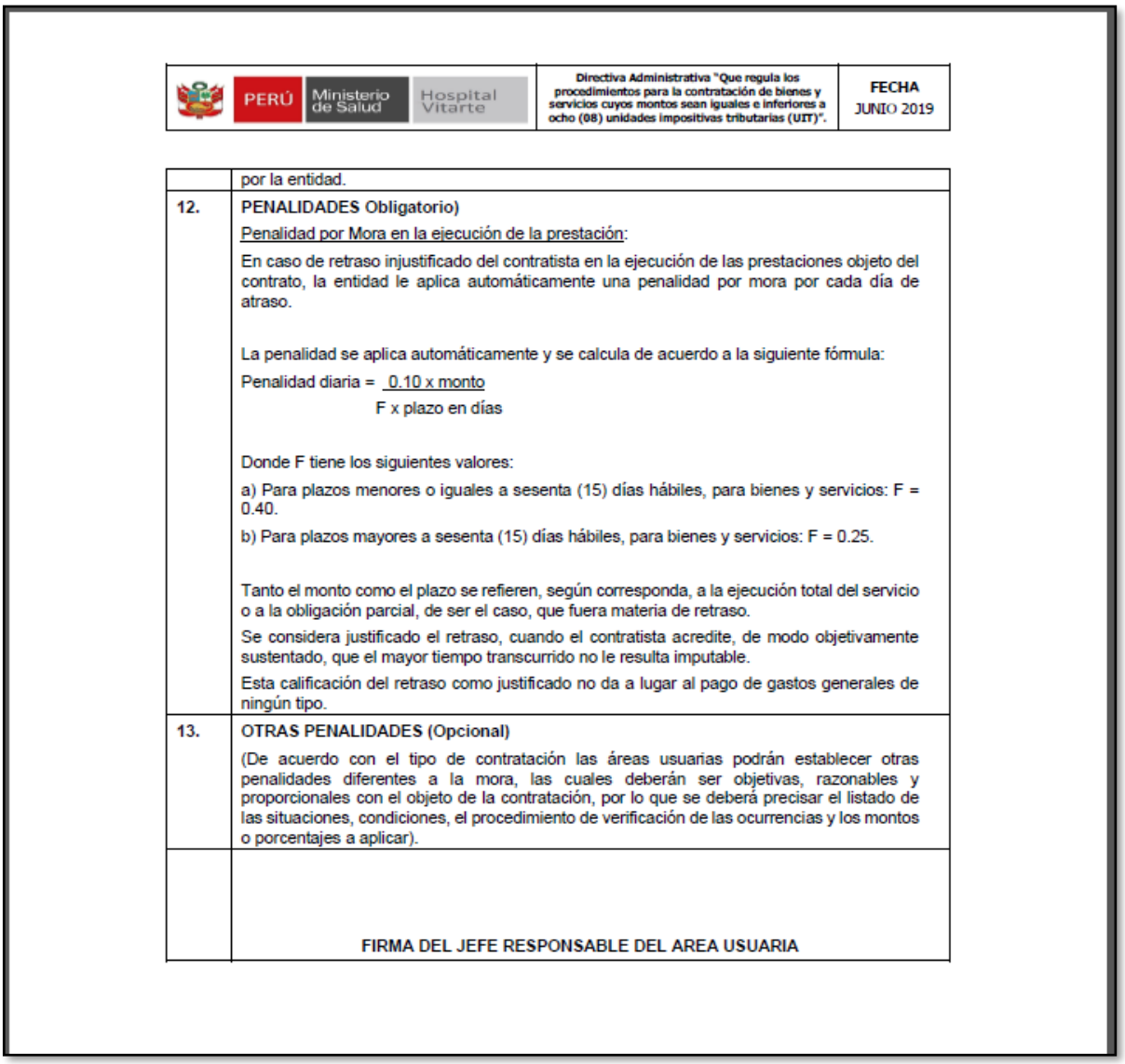
Unidad Orgánica / Área usuaria:	
Actividad del POI:	(Actividad / Meta programada en el Plan Operativo)
Denominación de la Contratación:	870100030010 – SERVICIO DE INTERNET
Pedido de Servicio N°	(Número del Pedido SIGA)

1.	**FINALIDAD PÚBLICA (Obligatorio)** El Hospital de baja complejidad de Vitarte requiere obtener el servicio de Internet para el registro de los documentos que hayan cumplido su vigencia administrativa en el Sistema de Archivo Documentario, asimismo acceso a los sistemas administrativos de la institución (SIGA, SIAF, OSCE, Trámite Documentario y Correo Institucional).
2.	**OBJETIVOS DE LA CONTRATACIÓN (Obligatorio)** **Objetivo General:** Se requiere obtener el servicio de acceso de Telefonía Fija e Internet para las conexiones múltiples de los usuarios finales. **Objetivo Específico:** - Integración del servicio de Internet con acceso a los sistemas administrativos de la institución. - Acceso a los sistemas administrativos de la institución y navegación a internet (SIGA, SIAF, OSCE, Trámite Documentario y Correo Institucional).
3.	**ALCANCE Y DESCRIPCIÓN DEL SERVICIO (Obligatorio)** El servicio de Acceso a Internet solicitado deberá contar con las siguientes características: **Enlace Principal y Secundario:** ✓ Acceso a Internet con un ancho de banda simétrico mínimo de 100 Mbps garantizado para su Sede Central ubicada en la Av. José Carlos Mariátegui 539 – Vitarte - Lima. Dicho servicio se contrata bajo la modalidad de 24 x 7 y por un período de 12 meses. ✓ El Medio físico para los enlaces deben ser Mikrotik u otro. **Características generales de Enlace:** ✓ El ISP deberá otorgarnos todos los permisos de administración del Router Mikrotik para futuros cambios y configuraciones. ✓ Sin perjuicio de lo señalado en forma precedente, el ISP deberá cumplir con los siguientes requerimientos: ✓ Disponibilidad de contar con equipos de reemplazo en caso de fallas o averías físicas. ✓ Los equipos de comunicación que serán implementados por el ISP correrán por cuenta del mismo y su interface LAN deberá ser igual o mayor a 1000Mbps. ✓ El ISP deberá reparar o reemplazar sin costo los equipos o componentes que sean necesarios para asegurar la prestación del servicio en caso de falla de los equipos suministrados.
4.	**REGLAMENTOS TECNICOS, NORMAS SANITARIAS Y OTRAS NORMAS (De Corresponder)** Es responsabilidad del contratista implementar las medidas dispuestas en el protocolo

Figura 28. TDR para la contratación de servicios – Parte 1

	sanitario sectorial para la prevención del Covid-19, estableciendo las acciones y responsabilidades de su personal asignado, dispuesto en el anexo IV de la resolución 0257-2020-MTC/01 del Ministerio de Transporte y Comunicaciones.
5.	**PRESTACIONES ACCESORIAS** **Gestión del Servicio:** ✓ El ISP deberá contar con una línea telefónica directa para la atención de un problema. ✓ El postor deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de atención, y personal de reparación de averías. Así mismo, deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten. ✓ El hospital se reserva la potestad de constatar la información presentada por el operador. ✓ Durante el período de prestación del servicio se evaluarán los tiempos de respuesta y la calidad del servicio, a fin de que el hospital determine las correcciones necesarias si fuera el caso. **Atención por averías:** ✓ Se entenderá por avería a una interrupción parcial o total del servicio, así como a una pérdida de la calidad del mismo. ✓ Toda actividad o provisión de bienes que tenga que ejecutar el postor para subsanar la avería será sin costo alguno para el hospital. ✓ El postor deberá contar con un centro de servicio instalado de tal manera que le asegure al hospital que se encuentra en condiciones de cumplir con lo estipulado en las bases. ✓ El Hospital solamente reportará las averías técnicas en el servicio a un único número telefónico, el cual será el punto de contacto con el ISP, permitiendo un adecuado control y seguimiento del servicio contratado. ✓ El Hospital podrá comunicarse con el servicio del ISP de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas.
6.	**REQUISITOS DE PROVEDOR (Obligatorio)** Prestación de personal técnico ante una falla de servicio o desastre de hardware, cantidad mínima de personal (1)
7.	**LUGAR Y PLAZO DE EJECUCION (Obligatorio)** El lugar de la ejecución de la prestación del servicio será en el Hospital Vitarte (Local Alquilado ubicado en José Carlos Mariátegui 539 Ate Vitarte – Lima), y el plazo de la ejecución del servicio no deberá exceder a 15 días hábiles, contados a partir de la firma del contrato.
8.	**ENTREGABLES (Obligatorio)** El proveedor esta en obligación de dejar un acta de conformidad sobre el equipo y servicio implementado.
9.	**CONFORMIDAD (Obligatorio)** La conformidad del servicio estará a cargo del Área de Archivo Central Documentario.
10.	**FORMA Y CONDICIONES DE PAGO (Obligatorio)** La forma de pago será de acuerdo a lo que formule el contrato con el proveedor del servicio.
11.	**RESPONSABILIDAD DEL CONTRATISTA** El contratista es el responsable por la calidad ofrecida y por los servicios ocultos del servicio ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada

Figura 29. TDR para la contratación de servicios – Parte 2



PERÚ Ministerio de Salud Hospital Vitarte	Directiva Administrativa "Que regula los procedimientos para la contratación de bienes y servicios cuyos montos sean iguales e inferiores a ocho (08) unidades impositivas tributarias (UIT)".	FECHA JUNIO 2019

	por la entidad.
12.	**PENALIDADES Obligatorio)** Penalidad por Mora en la ejecución de la prestación: En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula: Penalidad diaria = 0.10 x monto / F x plazo en días Donde F tiene los siguientes valores: a) Para plazos menores o iguales a sesenta (15) días hábiles, para bienes y servicios: F = 0.40. b) Para plazos mayores a sesenta (15) días hábiles, para bienes y servicios: F = 0.25. Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso. Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación del retraso como justificado no da a lugar al pago de gastos generales de ningún tipo.
13.	**OTRAS PENALIDADES (Opcional)** (De acuerdo con el tipo de contratación las áreas usuarias podrán establecer otras penalidades diferentes a la mora, las cuales deberán ser objetivas, razonables y proporcionales con el objeto de la contratación, por lo que se deberá precisar el listado de las situaciones, condiciones, el procedimiento de verificación de las ocurrencias y los montos o porcentajes a aplicar).
	FIRMA DEL JEFE RESPONSABLE DEL AREA USUARIA

Figura 30. TDR para la contratación de servicios – Parte 3

Especificaciones Técnicas (EETT) para la adquisición de bienes - Firewall FortiGate-100E (ANEXO 04)

PERÚ Ministerio de Salud Hospital Vitarte	Directiva Administrativa "Que regula los procedimientos para la contratación de bienes y servicios cuyos montos sean iguales e inferiores a ocho (08) unidades impositivas tributarias (UIT)".	FECHA JUNIO 2019

ESPECIFICACIONES TECNICAS (EETT) PARA LA ADQUISICION DE BIENES

Unidad Orgánica / Área usuaria:	
Actividad del POI:	(Actividad / Meta programada en el Plan Operativo)
Denominación de la Contratación:	952278320001 – EQUIPO DE SEGURIDAD PERIMETRAL FIREWALL FORTIGATE 100E
Pedido de Compra N°	(Número del Pedido SIGA)

1.	**FINALIDAD PÚBLICA (Obligatorio)** El Hospital de baja complejidad de Vitarte requiere obtener el equipo de red Firewall FortiGate-100E para la conexión VPN-SSL, asimismo acceso remoto a los recursos, aplicaciones y sistemas administrativos de la institución.
2.	**OBJETIVOS DE LA CONTRATACIÓN (Obligatorio)** **Objetivo General:** Lograr la conexión remota de los trabajadores del Hospital Vitarte mediante la modalidad de Teletrabajo mediante un túnel seguro y encriptado VPN-SSL para el acceso a los sistemas alojados en la red principal HV. **Objetivo Específico:** - El área o unidad orgánica lograra conectarse a los servicios internos del Hospital Vitarte - Garantizar la conexión segura mediante el túnel encriptado de la VPN mencionada
3.	**CARACTERISTICAS TECNICAS (Obligatorio)** La serie FortiGate-100E ofrece protección real e integral, conteniendo todos los beneficios de una UTM (Gestión Unificada de Amenazas) Fortinet. Proporciona aceleración de firewall en todos los tamaños de paquetes, aceleración de procesamiento de contenido UTM, acceso remoto seguro y VPN de alta velocidad para un rendimiento y protección superior. - Modelo: FortiGate-100E - Firewall Throughput (1518/512/64 byte UDP): 1.5 / 1.5 / 1.5 Gbps - Firewall Latency: 4 µs - Concurrent Sessions: 500,000 - New Sessions/Sec: 4,000 - IPS Throughput (HTTP / Enterprise Mix): 200 /41 Mbps - SSL Inspection Throughput: 32 Mbps - Application Control Throughput: 50 Mbps - NGFW Throughput: 23 Mbps - Threat Protection Throughput: 20 Mbps - Interfaces: 10x GE RJ45
4.	**REGLAMENTOS TECNICOS, NORMAS SANITARIAS Y OTRAS NORMAS (De Corresponder)** Es responsabilidad del contratista implementar las medidas dispuestas en el protocolo sanitario sectorial para la prevención del Covid-19, estableciendo las acciones y responsabilidades de su personal asignado, dispuesto en el anexo IV de la resolución 0257-2020-MTC/01 del Ministerio de Transporte y Comunicaciones.
5.	**ACONDICIONAMIENTO, MONTAJE O INSTALACIÓN (De Corresponder)** No se requiere el montaje del equipo por ser de gama media y de dimensión pequeña.

Figura 31. EETT para la adquisición de bienes – Parte 1

6.	**GARANTIA COMERCIAL (Obligatorio)** La garantía de hardware será ofrecida por el proveedor durante un año.
7.	**MUESTRAS** El proveedor deberá demostrar que el equipo cumple con todas las especificaciones técnicas descritas del producto.
8.	**PRESTACIONES ACCESORIAS** No se requieren prestaciones accesorias.
9.	**REQUISITOS DE PROVEDOR (De Corresponder)** Prestación de personal técnico ante una falla o desastre de hardware, cantidad mínima de personal (1)
10.	**LUGAR Y PLAZO DE ENTREGA (Obligatorio)** El lugar de la ejecución de la prestación del bien será en el Hospital Vitarte (Local Alquilado ubicado en José Carlos Mariátegui 539 Ate Vitarte – Lima), y el plazo de entrega del bien no deberá exceder a 15 días hábiles, contados a partir de la firma del contrato.
11.	**CANTIDAD Y CRONOGRAMA DE ENTREGAS (Obligatorio)** **Cantidad:** 1 **Cronograma:** En una sola entrega.

Descripción Ítem	**CANTIDAD SEGÚN ENTREGAS** (semanal, quincenal o mensual) (Debe ser definida por el área usuaria según necesidad)						
	1	2	3	4	5	6	TOTAL
Ítem 1	X						1
Ítem 2							

12.	**CONFORMIDAD (Obligatorio)** La conformidad del bien estará a cargo del Área de Archivo Central Documentario.
13.	**FORMA Y CONDICIONES DE PAGO (Obligatorio)** La forma de pago será de acuerdo a lo que formule el contrato con el proveedor del bien.
14.	**RESPONSABILIDAD DEL CONTRATISTA** El contratista es el responsable por la calidad ofrecida del bien ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la entidad.
15.	**PENALIDADES Obligatorio)** Penalidad por Mora en la ejecución de la prestación: En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula: Penalidad diaria = $\frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$ Donde F tiene los siguientes valores: a) Para plazos menores o iguales a sesenta (15) días hábiles, para bienes y servicios: F = 0.40. b) Para plazos mayores a sesenta (15) días hábiles, para bienes y servicios: F = 0.25. Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.

Figura 32. EETT para la adquisición de bienes – Parte 2

Requerimiento del usuario final:

Visualizando la tabla 3, se detalla requerimientos a nivel de usuarios, esto incluye métodos de recolección de información, en cuentas e interrogaciones de principales grupos con la finalidad de arrojar datos percibidos del usuario en relación a los servicios de red, considerando esencialmente tiempos en la escalabilidad, estabilidad y disponibilidad.

Tabla 4. Requerimiento del usuario final

REQUERIMINETO	OBJETIVO
Conexiones permanentes	Minimizar los errores sobre enlaces y nodos, optimizar el tiempo de recuperacion para reducir al minimo el tiempo de inactividad de los servicios de Comunicación
Accesibilidad de usuarios	Expandir la red para admitir a nuevos usuarios y aplicaciones sin afectar el rendimiento de los servicios de los usuarios.
Rapidez de acceso a los Sistemas informaticos	Mejorar los tiempos de respuesta al cargar los Sistemas alojados en los servidores del Hospital de Vitarte

Requerimiento para las aplicaciones y sistemas del HV:

En la Tabla 4, mostramos los requerimientos a nivel de aplicación de rendimiento intensivo que en su mayoría implican las tareas de traspaso o entrega, consultas y acceso a los datos de los distintos sistemas con los que cuenta el Hospital de Vitarte. Esta comunicación con los sistemas es primordial ya que los datos o acuses mantendrán una réplica bidireccional. No obstante, una aceptable cantidad de datos extraviados, trafico clasificado, fluidez de la conexión, son requisitos importantes para estos sistemas y sus consultas.

Tabla 5. Requerimiento para las aplicaciones

REQUERIMINETO	OBJETIVO
Pérdida de paquetes aceptables	Hacer fiable los datos de unidifusión IP que se generan o envían los trabajadores remotos.
Priorización de tráfico	Enfrentar los requerimientos de sistemas sensibles a pérdidas, retrasos y variaciones que permiten la preferencia de flujos de aplicación critica en el ancho de banda disponible.
Seguridad	Control de acceso a la red de datos y sistemas, asegurar el metodo de doble factor de autenticación con la finalidad de proteger la informacion que es el recurso mas valioso de la entidad.

Requerimientos de Infraestructura:

Un requerimiento importante para la infraestructura de la red del Hospital de Vitarte es que el Servicio de Comunicación sea escalable y con tolerancia a soportar las conexiones remotas de más de 100 trabajadores simultáneos, para este escenario se requiere equipos que permitan esta redundancia ante posibles fallas lógicas.

Análisis técnico

- ✓ **Escalabilidad**

El despliegue de la solución a implementar cuenta con capacidad aproximada de 100 usuarios VPN activos simultáneamente, pero con un crecimiento futuro y escalable de 500 usuarios simultáneos que soporta el equipo según las especificaciones técnicas ya descritas en el Datasheet del producto en sí.

- ✓ **Disponibilidad**

Dado que el servicio es imprescindible, se encuentra activo las 24 horas del día, pero se aplicarán políticas con horarios de acceso para mantener el cumplimiento de los roles de cada trabajador por unidad o servicio dentro del Hospital de Vitarte.

- ✓ **Rendimiento**

La solución a implementar cuenta con la adaptabilidad necesaria para soportar un futuro crecimiento de usuarios y se garantice la conexión simultanea sin interrupciones.

- ✓ **Seguridad**

La confidencialidad e integridad de los datos viajaran seguros, ya que el túnel VPN será encriptado y contará con un previo método de acceso añadiendo el método de doble factor de autenticación.

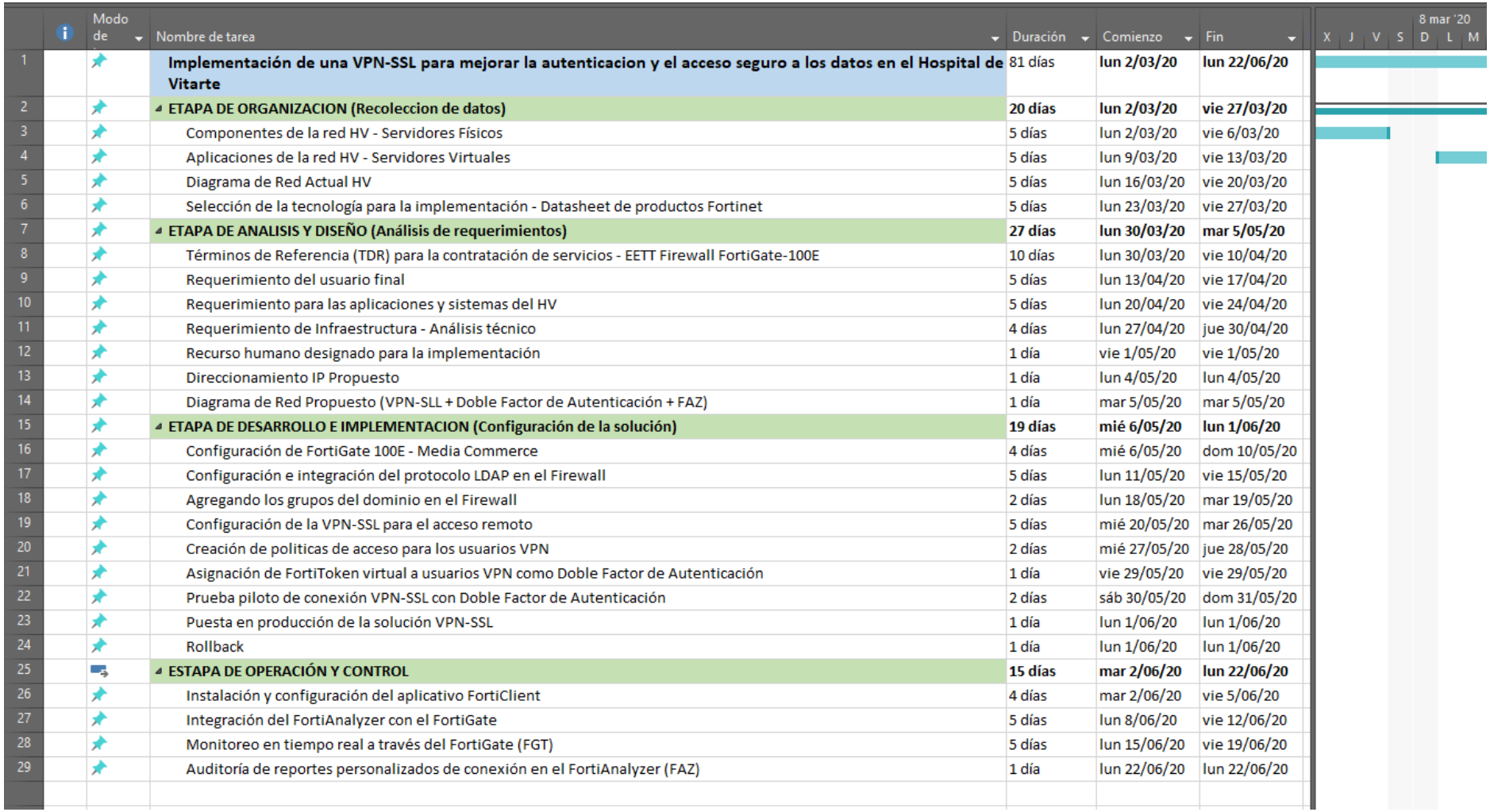
Recurso humano designado para la implementación:

N°	NOMBRE	DESCRIPCIÓN
1	Roberto Flores Ayqui	Especialista en Redes y Comunicaciones NSE1, NSE2, NSE3, NSE4

Plan de trabajo

Este plan de trabajo se ejecutará mediante un diagrama de Gantt, visualizando así las actividades del proyecto y su duración por cada etapa, fechas según lo planificado considerando que es un diagrama planeado y mientras existan modificaciones en el tiempo de las actividades pasará a ser un diagrama ejecutado.

Cronograma de Actividades – Etapas para la implementación VPN-SSL en el Hospital de Vitarte



	Modo de	Nombre de tarea	Duración	Comienzo	Fin
1		**Implementación de una VPN-SSL para mejorar la autenticacion y el acceso seguro a los datos en el Hospital de Vitarte**	81 días	**lun 2/03/20**	**lun 22/06/20**
2		**ETAPA DE ORGANIZACION (Recoleccion de datos)**	**20 días**	**lun 2/03/20**	**vie 27/03/20**
3		Componentes de la red HV - Servidores Físicos	5 días	lun 2/03/20	vie 6/03/20
4		Aplicaciones de la red HV - Servidores Virtuales	5 días	lun 9/03/20	vie 13/03/20
5		Diagrama de Red Actual HV	5 días	lun 16/03/20	vie 20/03/20
6		Selección de la tecnología para la implementación - Datasheet de productos Fortinet	5 días	lun 23/03/20	vie 27/03/20
7		**ETAPA DE ANALISIS Y DISEÑO (Análisis de requerimientos)**	**27 días**	**lun 30/03/20**	**mar 5/05/20**
8		Términos de Referencia (TDR) para la contratación de servicios - EETT Firewall FortiGate-100E	10 días	lun 30/03/20	vie 10/04/20
9		Requerimiento del usuario final	5 días	lun 13/04/20	vie 17/04/20
10		Requerimiento para las aplicaciones y sistemas del HV	5 días	lun 20/04/20	vie 24/04/20
11		Requerimiento de Infraestructura - Análisis técnico	4 días	lun 27/04/20	jue 30/04/20
12		Recurso humano designado para la implementación	1 día	vie 1/05/20	vie 1/05/20
13		Direccionamiento IP Propuesto	1 día	lun 4/05/20	lun 4/05/20
14		Diagrama de Red Propuesto (VPN-SLL + Doble Factor de Autenticación + FAZ)	1 día	mar 5/05/20	mar 5/05/20
15		**ETAPA DE DESARROLLO E IMPLEMENTACION (Configuración de la solución)**	**19 días**	**mié 6/05/20**	**lun 1/06/20**
16		Configuración de FortiGate 100E - Media Commerce	4 días	mié 6/05/20	dom 10/05/20
17		Configuración e integración del protocolo LDAP en el Firewall	5 días	lun 11/05/20	vie 15/05/20
18		Agregando los grupos del dominio en el Firewall	2 días	lun 18/05/20	mar 19/05/20
19		Configuración de la VPN-SSL para el acceso remoto	5 días	mié 20/05/20	mar 26/05/20
20		Creación de politicas de acceso para los usuarios VPN	2 días	mié 27/05/20	jue 28/05/20
21		Asignación de FortiToken virtual a usuarios VPN como Doble Factor de Autenticación	1 día	vie 29/05/20	vie 29/05/20
22		Prueba piloto de conexión VPN-SSL con Doble Factor de Autenticación	2 días	sáb 30/05/20	dom 31/05/20
23		Puesta en producción de la solución VPN-SSL	1 día	lun 1/06/20	lun 1/06/20
24		Rollback	1 día	lun 1/06/20	lun 1/06/20
25		**ESTAPA DE OPERACIÓN Y CONTROL**	**15 días**	**mar 2/06/20**	**lun 22/06/20**
26		Instalación y configuración del aplicativo FortiClient	4 días	mar 2/06/20	vie 5/06/20
27		Integración del FortiAnalyzer con el FortiGate	5 días	lun 8/06/20	vie 12/06/20
28		Monitoreo en tiempo real a través del FortiGate (FGT)	5 días	lun 15/06/20	vie 19/06/20
29		Auditoría de reportes personalizados de conexión en el FortiAnalyzer (FAZ)	1 día	lun 22/06/20	lun 22/06/20

Figura 33. Diagrama de Actividades según Etapas del Proyecto

Se desarrolló un diseño detallado que comprenda requerimientos técnicos y de negocio, obtenidos como plan de proyecto que fue actualizado mediante un cronograma de actividades más granular para la implementación de la propuesta.

Tabla 6. Cronograma de Actividades por Etapas

CRONOGRAMA DE ACTIVIDADES POR ETAPA (Implementación de una VPN-SSL para mejorar la autenticacion y el acceso seguro a los datos en el Hospital de Vitarte)
ETAPA DE ORGANIZACIÓN
Componentes de la Red HV - Servidores Fisicos
Aplicaciones de la Red HV - Servidores Virtuales
Diagrama de Red Actual HV
Selección de la tecnología para la implementación
ETAPA DE ANÁLISIS Y DISEÑO
Analisis de Requerimientos (TDR y ETT)
Requerimiento del usuario final
Requerimiento para las aplicaciones y sistmas del HV
Requerimiento de infraestructura (Análisis Técnico)
Recurso humano designado para la implementación
Modelo de Negocio
Direccionamiento IP propuesto
Diagrama de Red Propuesto (VPN-SLL + Doble Factor de Autenticación + FAZ)
ETAPA DE DESARROLLO E IMPLEMENTACIÓN
Configuracion del FortiGate-100E
Configuracion e integracion del protocolo LDAP en el Firewall
Agregando los grupos del dominio en el Firewall
Configuracion de la VPN-SSL para el acceso remoto
Creacion de politicas de acceso para los usuarios VPN
Asignación de FortiToken virtual a usuarios VPN como Doble Factor de Autenticación
Prueba piloto de conexión VPN-SSL con metodo de Doble Factor de Autenticación
ETAPA DE OPERACIÓN Y CONTROL
Instalación y configuración del aplicativo FortiClient
Integración del FortiAnalyzer con el FortiGate
Monitoreo en tiempo real a través del FortiGate (FGT)
Auditoria de reportes personalizados de conexión en el FortiAnalyzer (FAZ)

Modelo de negocio

El modelo de negocio inicia con una evaluación de la cantidad de usuarios o trabajadores que contaran con esta modalidad según la unidad o servicio del mismo hospital de Vitarte.

Áreas Involucradas y cantidad de trabajadores remotos:

- CONSULTORIOS EXTERNOS (10)
- EMERGENCIAS (5)
- FARMACIA (10)
- JEFATURAS (10)
- LOGISTICA (5)
- PLANEAMIENTO (3)
- ECONOMIA (7)
- VENTANILLAS (10)
- ESTADISTICA E INFORMATICA (10)
- OTRAS UNIDADES – AREAS – SERVICIOS (10)

Direccionamiento IP propuesto

Para la conexión propuesta el esquema del direccionamiento IP se basa en tres grupos:

Tabla 7. Direccionamiento IP para la conexión.

NOMBRE	RED	MASCARA	PUERTA DE ENLACE
RED INTERNA	192.168.20.0	255.255.255.0	192.168.20.1
SERVIDORES	172.16.0.0	255.255.0.0	172.16.1.2
SSLVPN_TUNNEL_ADDR1	10.212.134.50-10.212.134.250	255.255.255.255	ssl.root
WAN 1	179.43.87.112	255.255.255.248	179.43.87.113
WAN 2	179.43.87.128	255.255.255.240	179.43.87.129

Diagrama de Red propuesto – VPN-SLL + Doble Factor de Autenticación FTA + FAZ

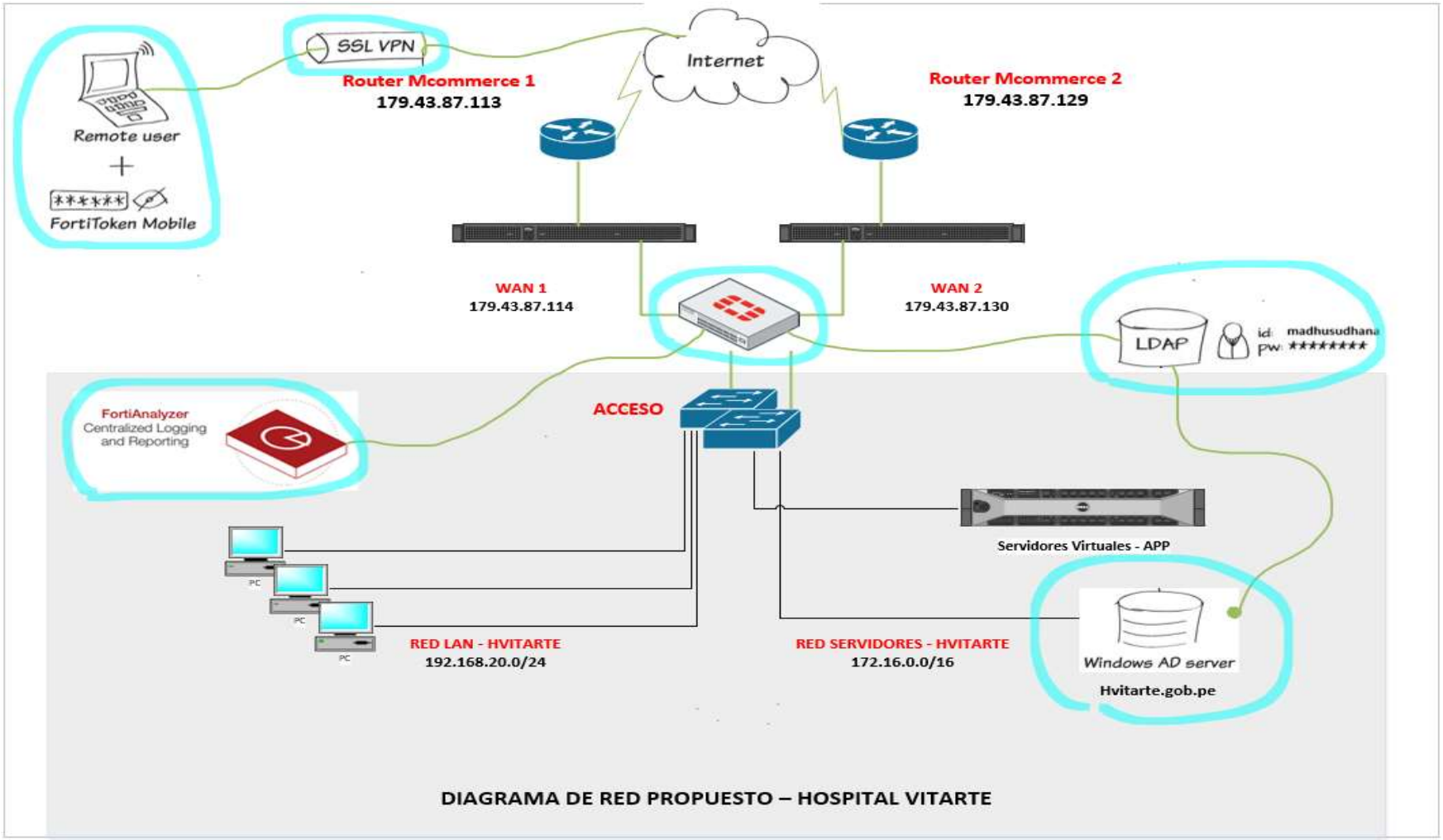


Figura 34. Diagrama de red propuesto para el Hospital de Vitarte

3.3.ETAPA DE DESARROLLO E IMPLEMENTACIÓN

A partir de esta etapa se lleva a cabo la instalación y configuración del equipo FortiGate-100E y la solución. En términos de proyecto el plan de trabajo deber ser cumplido, previamente acordado y aprobado por los miembros del equipo. El tiempo evaluado y documentado debe proveer un plan de contingencia, así como su respectivo rollback en caso de fallo general.

Configuración del FortiGate-100E

El proveedor de internet Media Commerce que brinda el servicio de internet al Hospital de Vitarte, cuenta con dos enlaces redundantes los cuales aprovecharemos para configurar la redundancia de internet en el FortiGate-100E propuesto para esta solución, por medio de la tecnología SD-WAN podremos unificar así dos enlaces físicos (WAN 1 y WAN 2) para crear la interfaz virtual SD-WAN como solución redundante de Internet para la navegación de los usuarios finales.

PASO 01: Para ello al ingresar al Firewall FortiGate-100E declararemos los puertos WAN (Enlaces de internet Principal y Redundante) así como su ruta estática de salida a Internet.

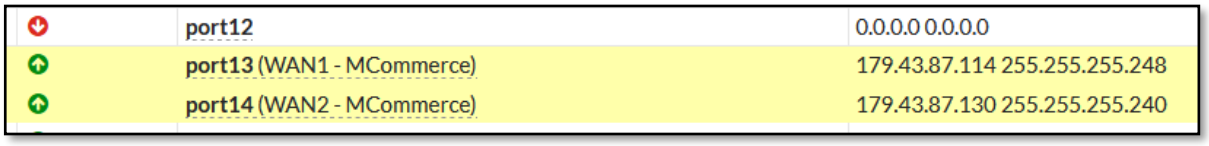


Figura 35. Configuración de los puertos WAN en el FGT-100E

PASO 02: Seguidamente configuramos la SD-WAN como se observa en la siguiente imagen, agregando a los puertos que serán los miembros de esta nueva interfaz.

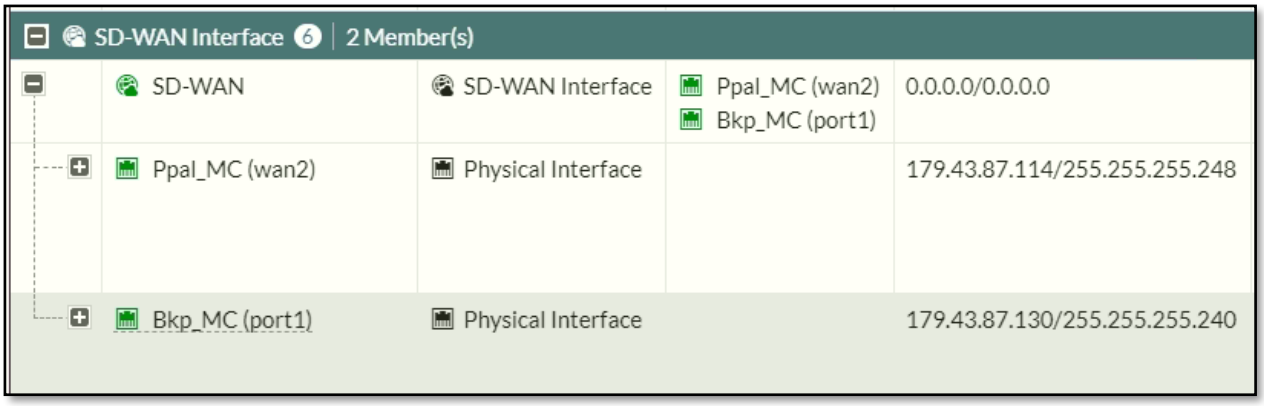


Figura 36. Creación de la interfaz SD-WAN en el FGT-100E

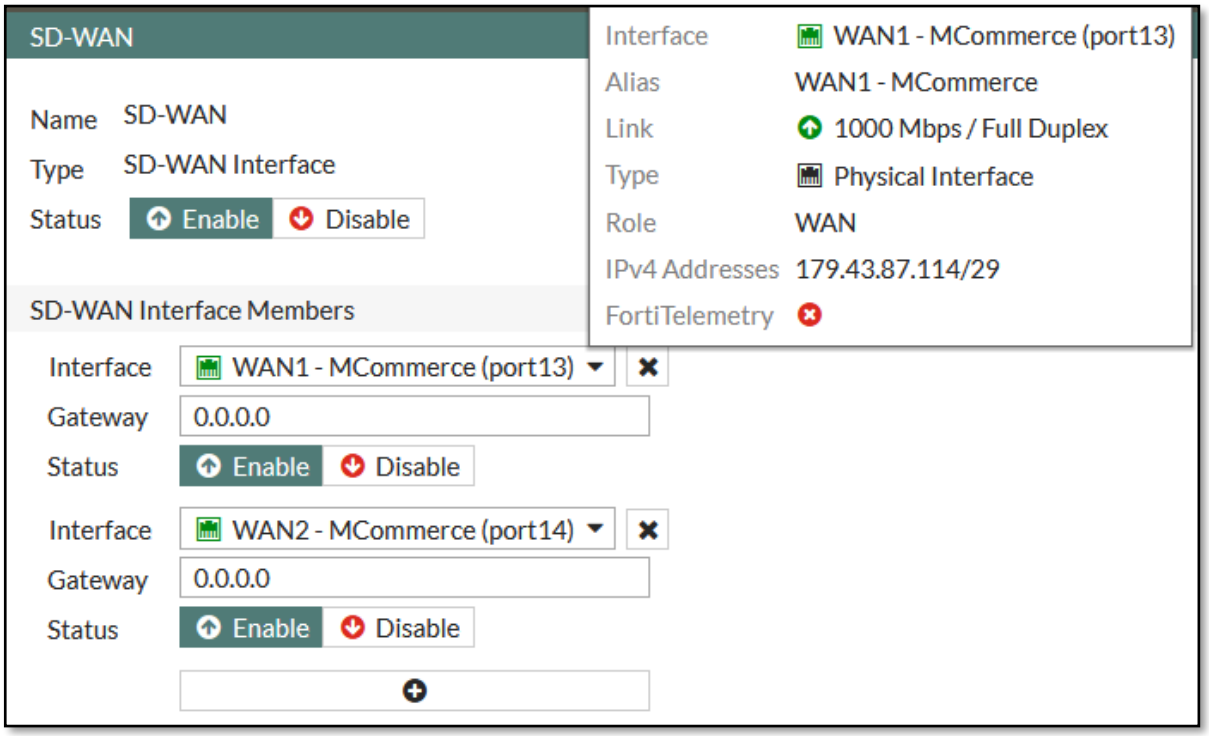


Figura 37. Ruta por defecto de la SD-WAN en el FGT-100E

PASO 03: El volumen de ancho de banda SD-WAN será proporcionalmente dividido para la subida y bajada de velocidad contratada por los enlaces de Internet como se aprecia en la figura de abajo.

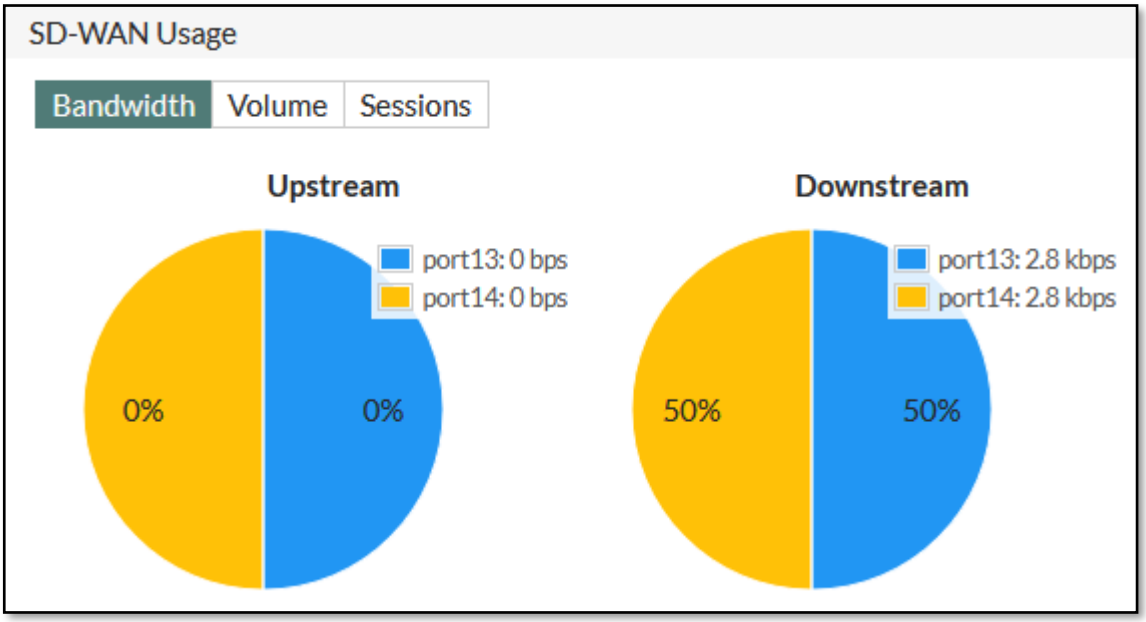


Figura 38. Distribución del Ancho de banda mediante la SD-WAN

PASO 04: Para ello en el servidor de dominio Active Directory ya debemos tener estructurada una relación de grupos del dominio que participarán y serán autorizados en esta conexión VPN para el teletrabajo en el Hospital de Vitarte tal como se puede observar en la siguiente figura del árbol de la entidad.

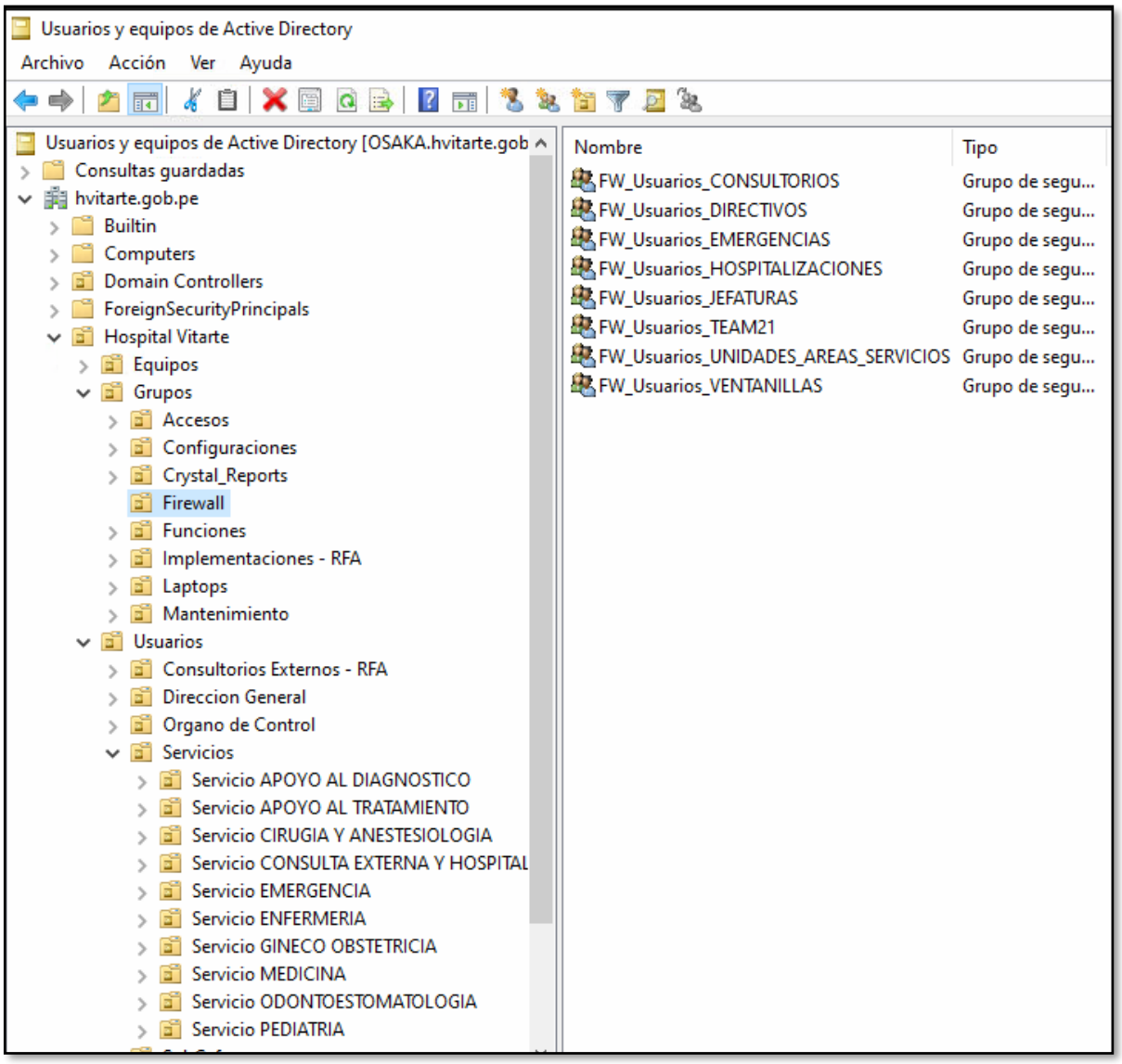


Figura 38-1. Grupos VPN declarados en el Active Directory para el Teletrabajo

Configuración e integración del protocolo LDAP en el Firewall

PASO 01: Para configurar la unidad FortiGate para la autenticación LDAP tenemos los siguientes pasos:

1. Vaya a Usuario y dispositivo -> Autenticación -> Servidores LDAP y seleccione Crear nuevo.
2. Ingrese un nombre para el servidor LDAP.
3. En Nombre / IP del servidor, ingrese el FQDN o la dirección IP del servidor.
4. Si es necesario, cambie el número de puerto del servidor. El puerto predeterminado es 389.
5. Introduzca el Identificador de nombre común (20 caracteres como máximo), cn es el predeterminado y la mayoría de los clientes utilizarán SAMAccountName. Cn es un nombre común que es un nombre para mostrar y SAMAccountName es el nombre de inicio de sesión (en referencia al servidor LDAP de Windows).
6. Para el nombre distinguido, haga clic en examinar y seleccione el dominio principal (seleccione el dominio una vez que ingrese el nombre de usuario y la contraseña según los pasos 8 y 9)
7. En Tipo de enlace, seleccione Regular.
8. En Nombre de usuario, ingrese el nombre del administrador LDAP junto con el dominio.
9. En Contraseña, ingrese la contraseña del administrador LDAP.
10. Seleccione Aceptar.

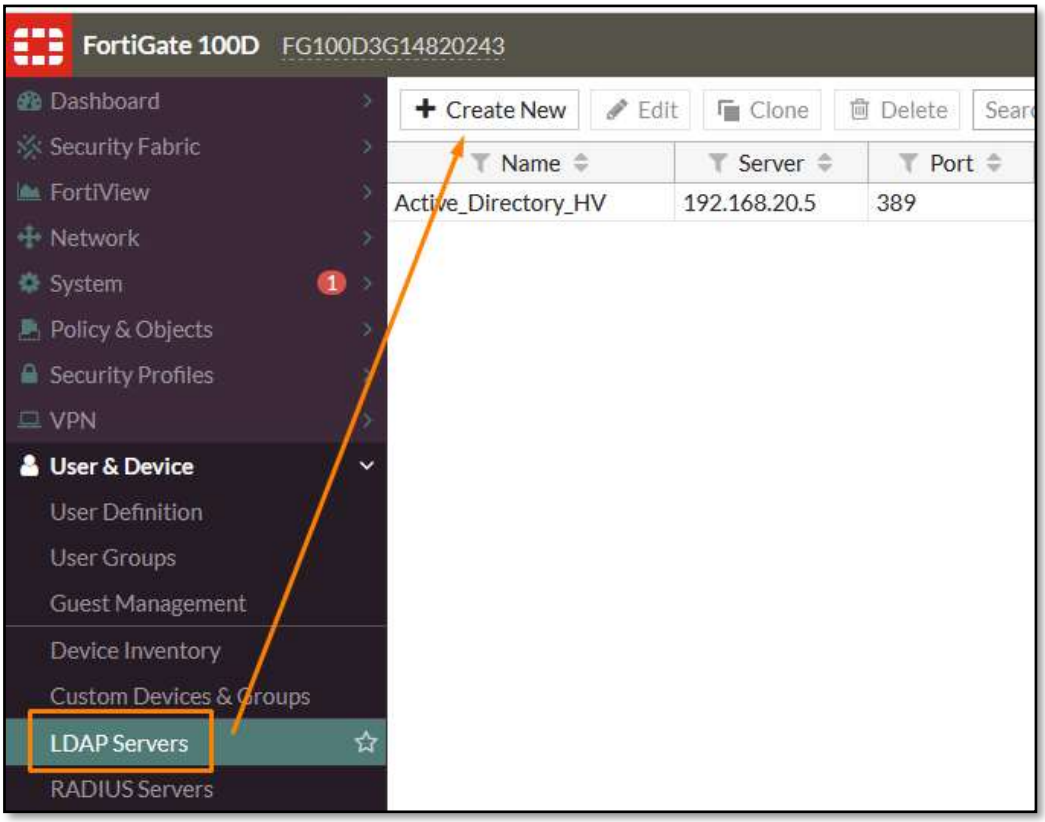


Figura 39. Creación e integración del protocolo LDAP en el FortiGate

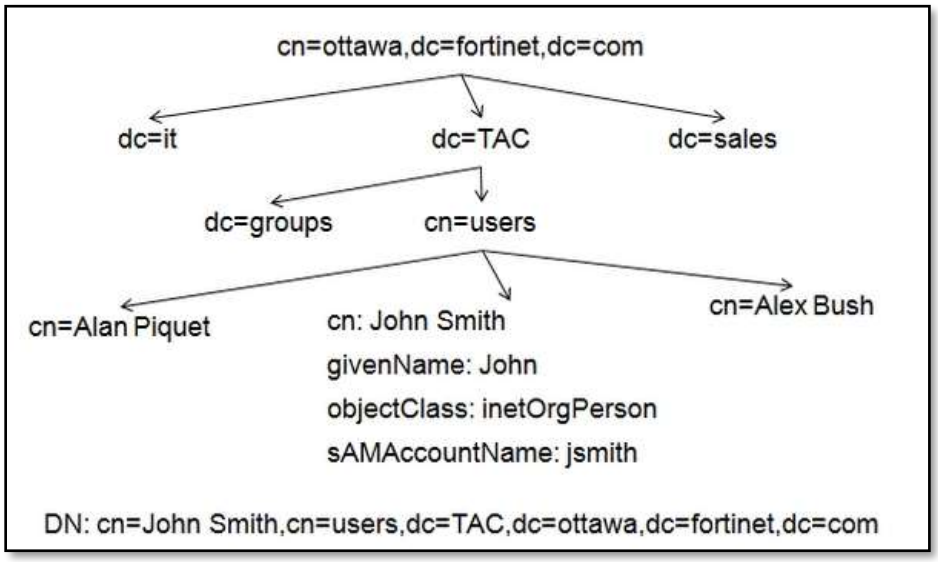


Figura 40. Ejemplo de una estructura LDAP

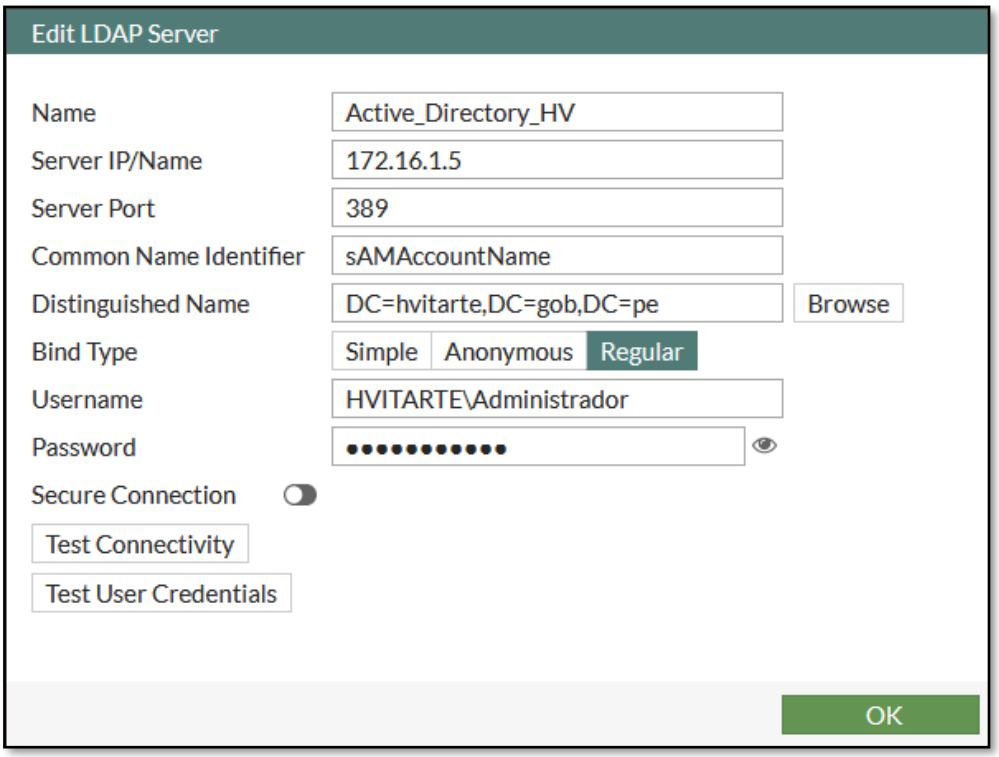


Figura 41. Parámetros del protocolo LDAP en el FortiGate

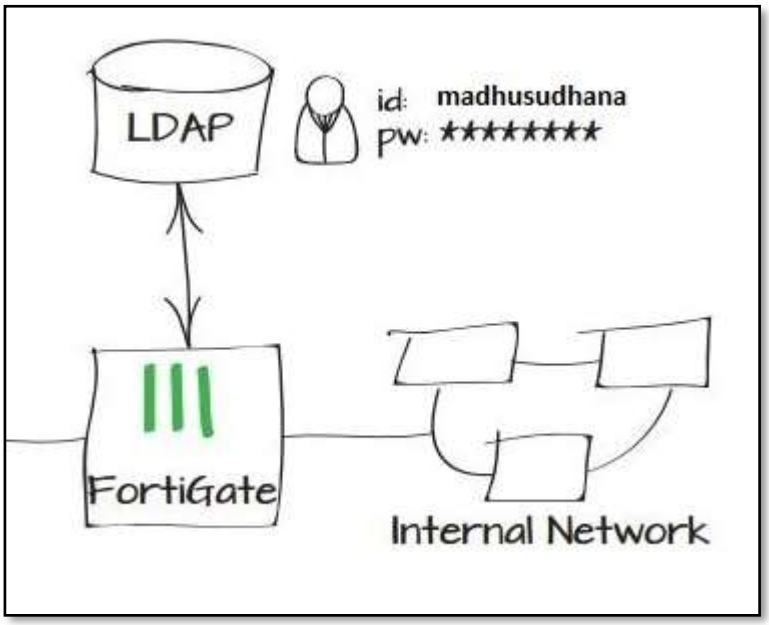


Figura 42. Representación del protocolo LDAP como BD en el FortiGate

PASO 02: Al seleccionar en “Browse” podremos ya ver reflejada la información del árbol del dominio del Hospital de Vitarte, junto a todos sus grupos y unidades organizativas existentes.

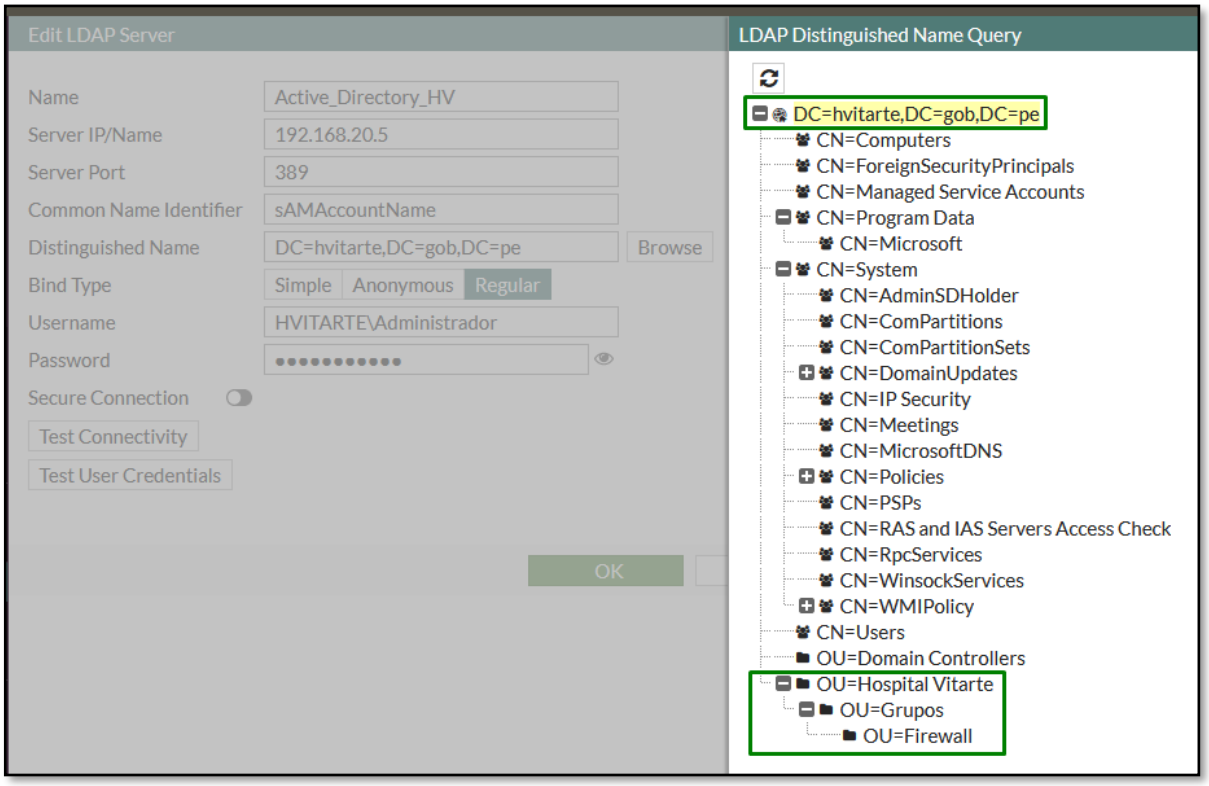


Figura 43. Base de datos LDAP ya sincronizada en el Firewall

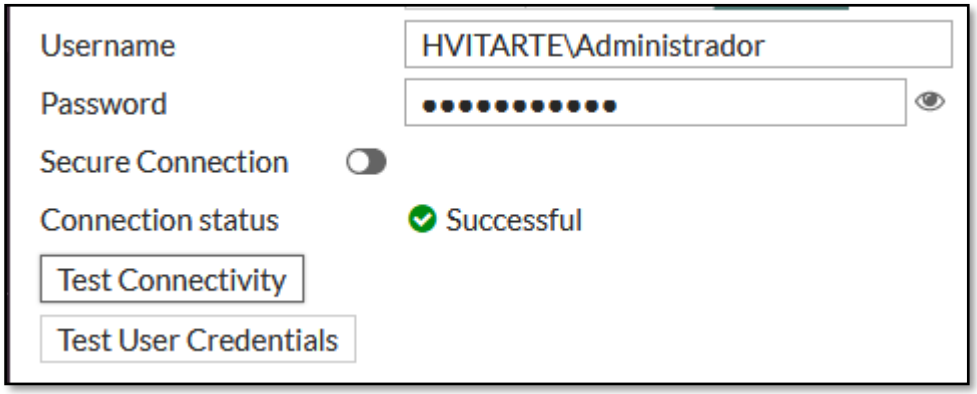


Figura 44. Test de conectividad contra el AD

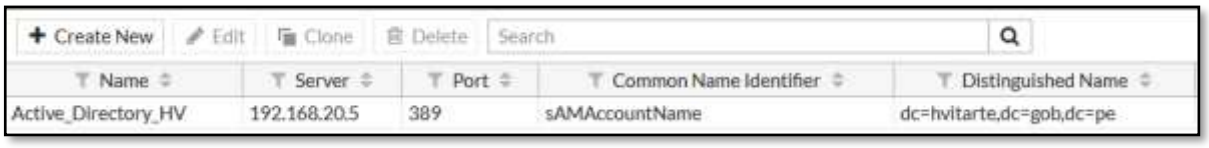


Figura 45. Registro correcto del LDAP Server en el FortiGate

Agregando a los grupos del dominio en el Firewall

Para lograr este punto seleccionaremos los grupos que ya fueron creados y estructurados en el Directorio Activo para que formen parte de la conexión VPN de acceso propuesta desde un principio, incluso se puede observar en la imagen que el grupo **"FW_Usuarios_CONSULTORIOS"** ya está seleccionado.

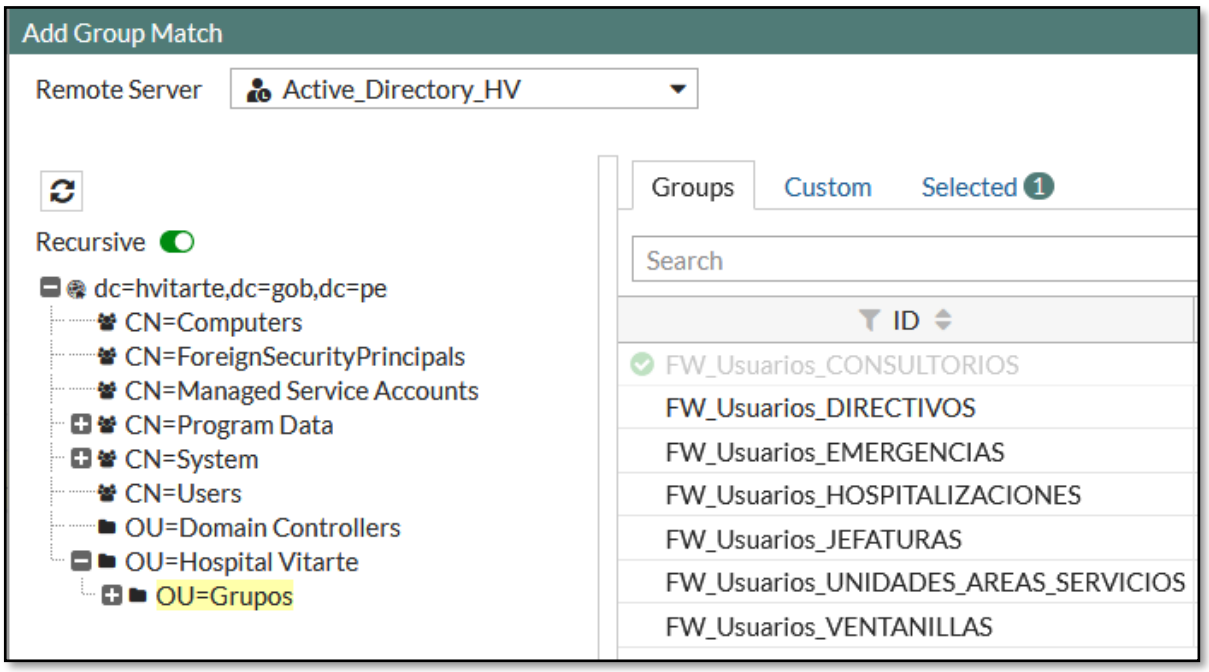


Figura 46. Agregando grupos VPN en relación al AD

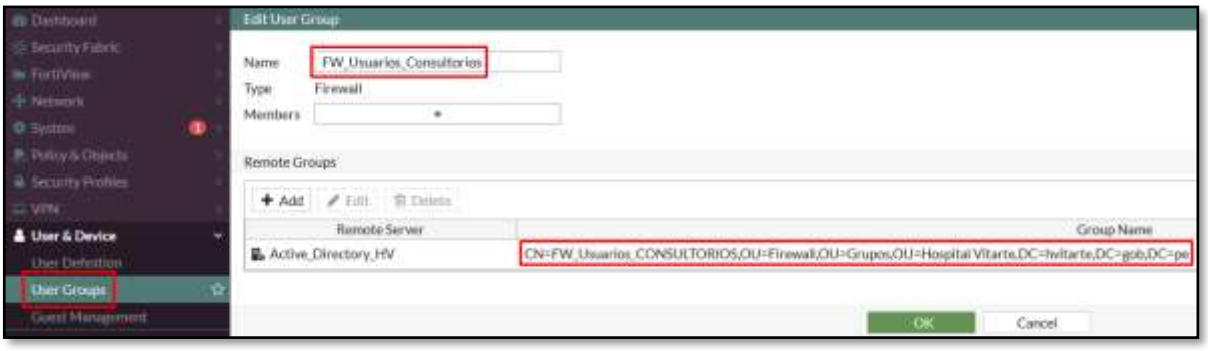


Figura 47. Creación correcta del grupo de acceso VPN

Configuración de la VPN-SSL para el acceso remoto

PASO 1: En el apartado **"SSL-VPN Portals"** crearemos un perfil para el túnel VPN asignado para nuestra solución, en el cual agregaremos nuestra red LAN con su segmento respectivo y el pool de direcciones privadas que recibirán nuestros clientes VPN desde el exterior.

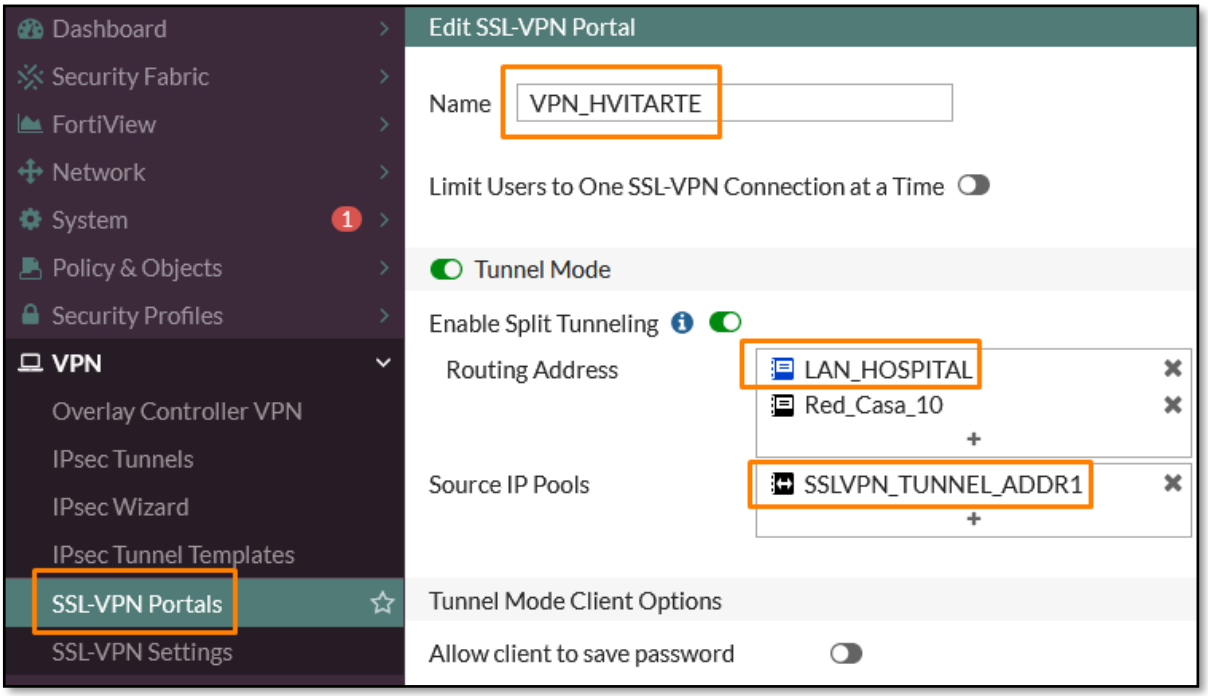


Figura 48. Configuración del portal VPN-SSL

PASO 2: Luego nos dirigimos al apartado **"SSL-VPN Settings"** en el cual asignaremos los puertos WAN que actualmente son miembros de la SD-WAN creada inicialmente, esto con el fin de que el acceso VPN sea mediante cualquiera de las 2 ip publicas configuradas con sus políticas respectivas.

Figura 49. Configuración de interfaces WAN de escucha

PASO 3: Continuando con el apartado, vamos a personalizar el puerto de escucha VPN para que no haga conflictos con el acceso HTTPS que ya tiene por defecto la página web de administración del mismo FortiGate, para ello cambiaremos el puerto **443 al 10443**, el cual más adelante será considerado en la configuración del aplicativo cliente en los equipos de acceso remoto como resultado.

PASO 4: Otro punto a considerar es seleccionar la opción **"Permitir el acceso desde cualquier host"** y en la autenticación agregaremos a nuestro grupo LDAP ya generado anteriormente como se puede observar en la imagen a detalle.

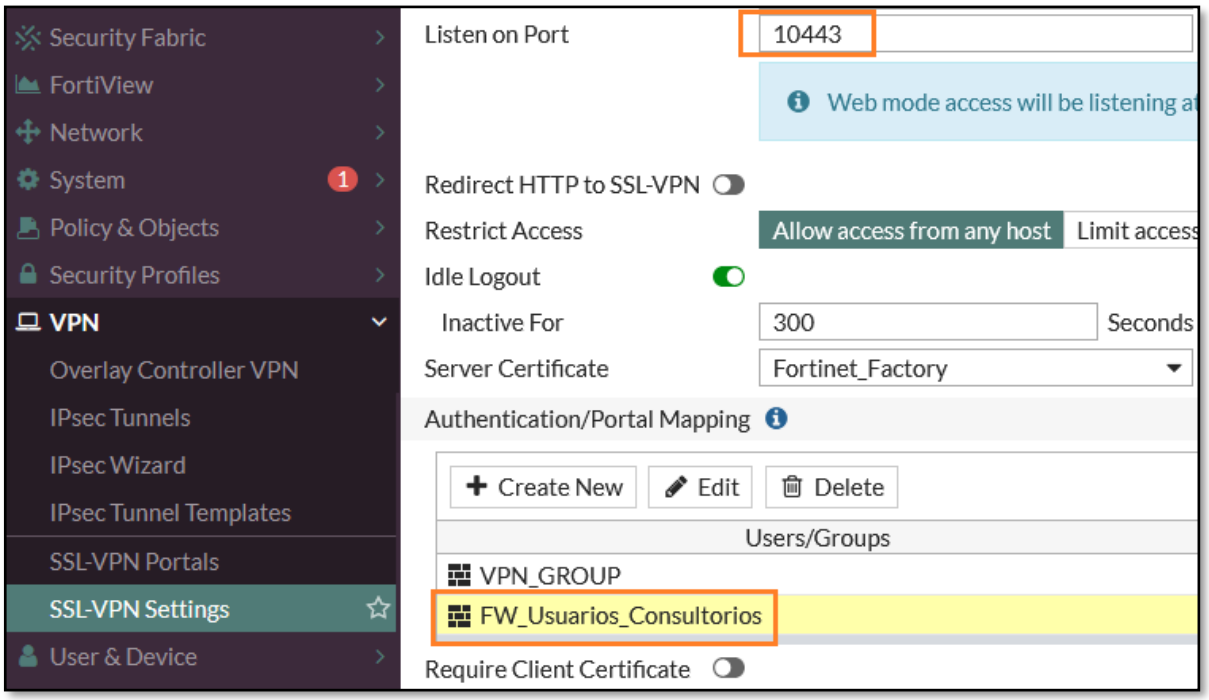


Figura 50. Personalizando puerto de escucha 10443

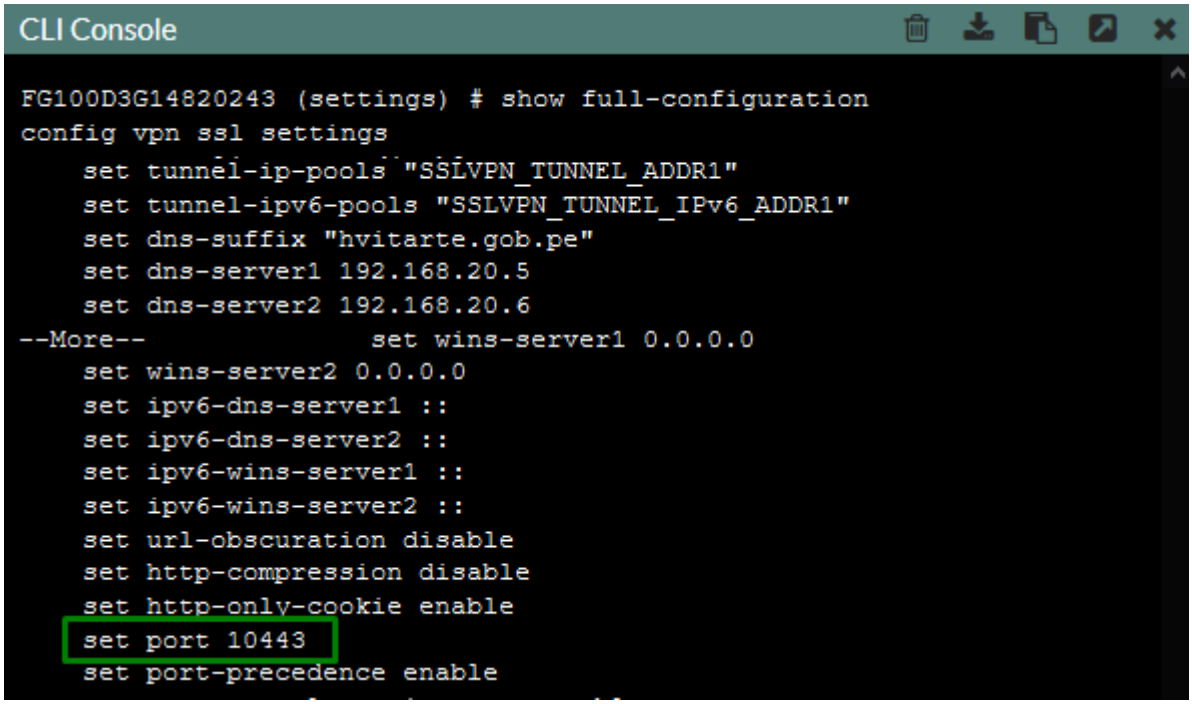


Figura 50. Verificación del puerto 10443 por la CLI

Creación de políticas de acceso para los usuarios VPN

Para terminar de configurar la VPN-SSL de acceso remoto, debemos de crear las reglas o políticas para que los equipos que se conecten a través de la VPN siguiendo los pasos detallados a continuación:

PASO 1: Iremos al apartado **"IPv4 Policy"** y crearemos una política agregando los campos de origen, red interna del Hospital de Vitarte, campo de destino, objetos previamente declarados, horario, servicio y el NAT habilitado, ya que para las demás que quisiéramos personalizar sería exactamente igual como se observa en la figura.

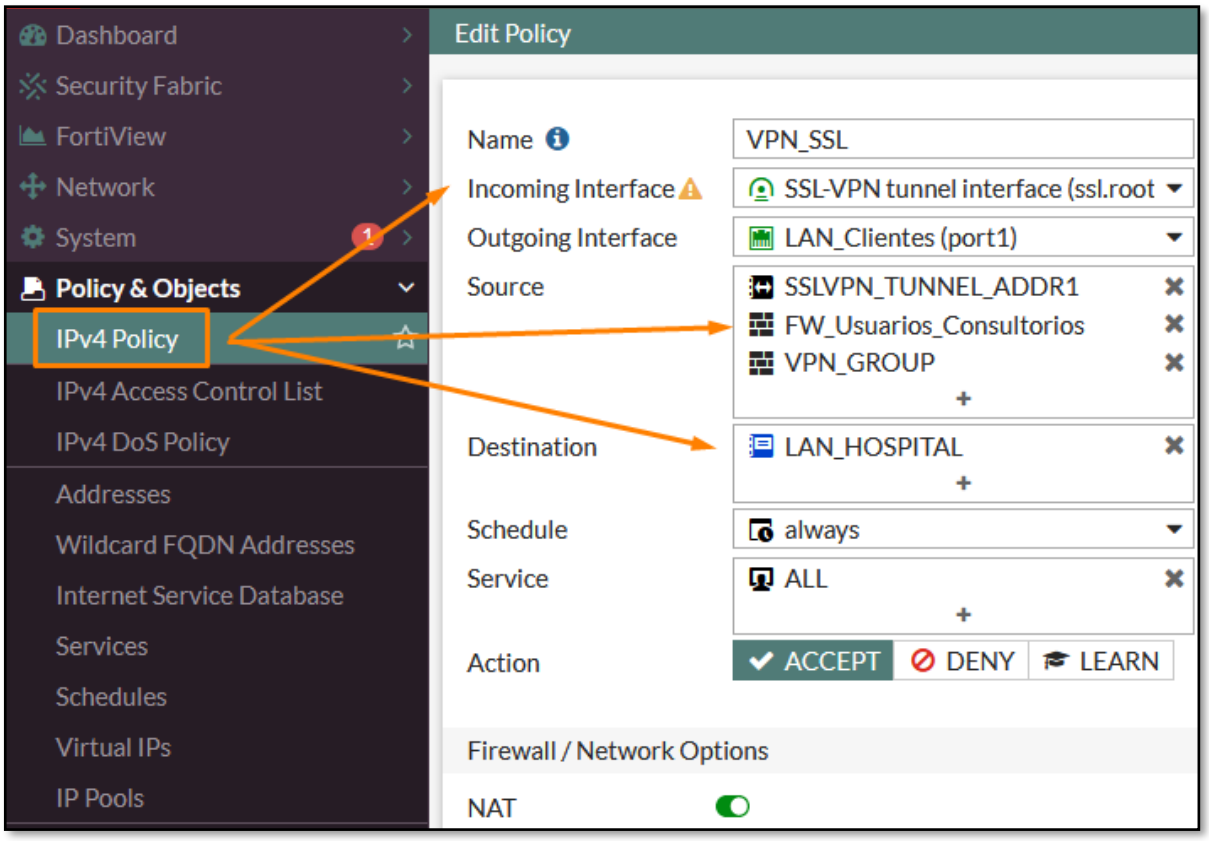


Figura 51. Política de acceso para los usuarios VPN

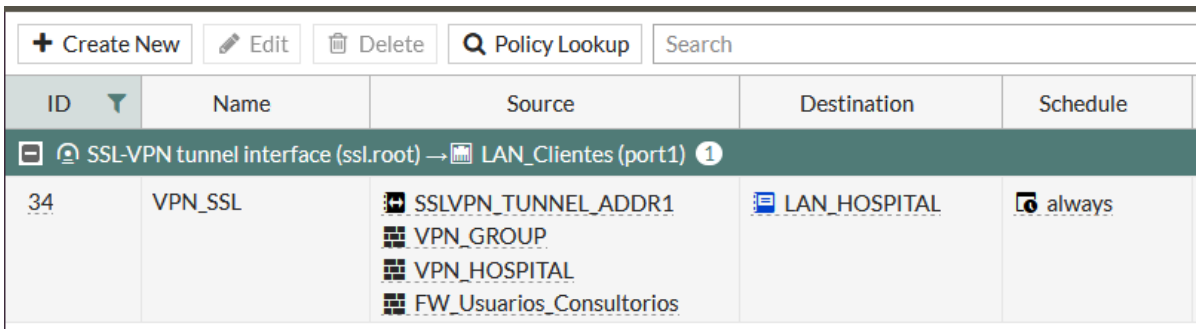


Figura 52. Resumen de la política creada para el acceso VPN

Asignación de FortiToken virtual a usuarios VPN como Doble Factor de Autenticación

PASO 1: Inicialmente desde la pestaña **"User definition"** del FortiGate importaremos un usuario del AD que fue configurado ya anteriormente mediante el protocolo LDAP en el mismo Firewall, seleccionamos la opción **"Remote LDAP User".**

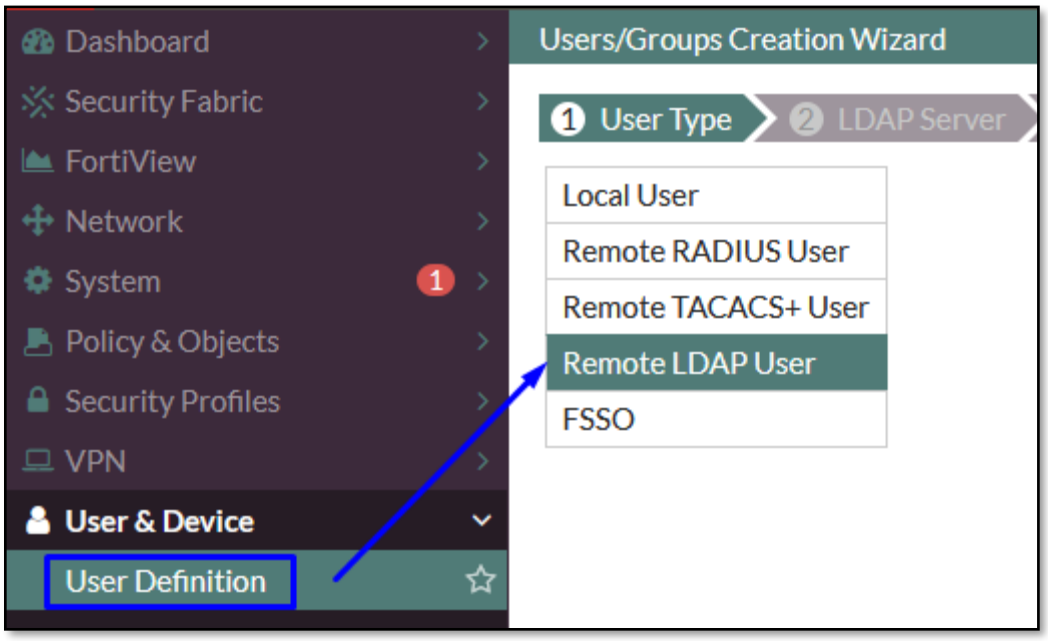


Figura 53. Declaración del usuario remoto LDAP

PASO 2: Seguidamente seleccionaremos nuestro único Directorio Activo que ya habíamos agregado por LDAP, es más al sombrear veremos los detalles de nuestro servidor y su configuración, le damos en siguiente.

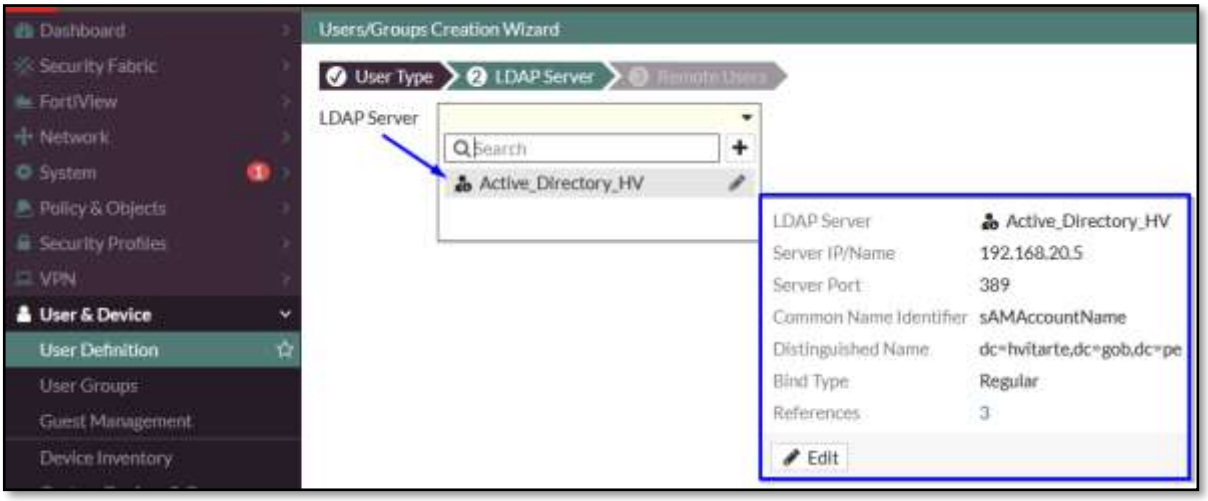


Figura 54. Seleccionando LDAP Server

PASO 3: Buscamos por la pestaña **"Users"** la cual filtrará cualquier usuario del dominio que exista en el AD, seleccionamos el usuario, damos click derecho y por último la opción asignar.

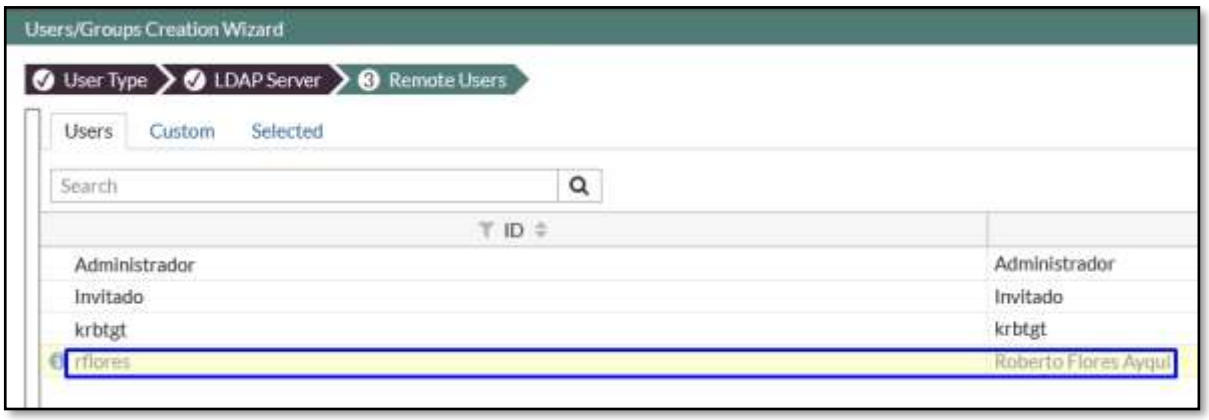


Figura 55. Búsqueda y selección de usuarios por LDAP Server

PASO 4: Damos en aplicar y veremos que nuestro usuario del AD ya está reflejado en el apartado "User Definition" con el estado **"LDAP"**

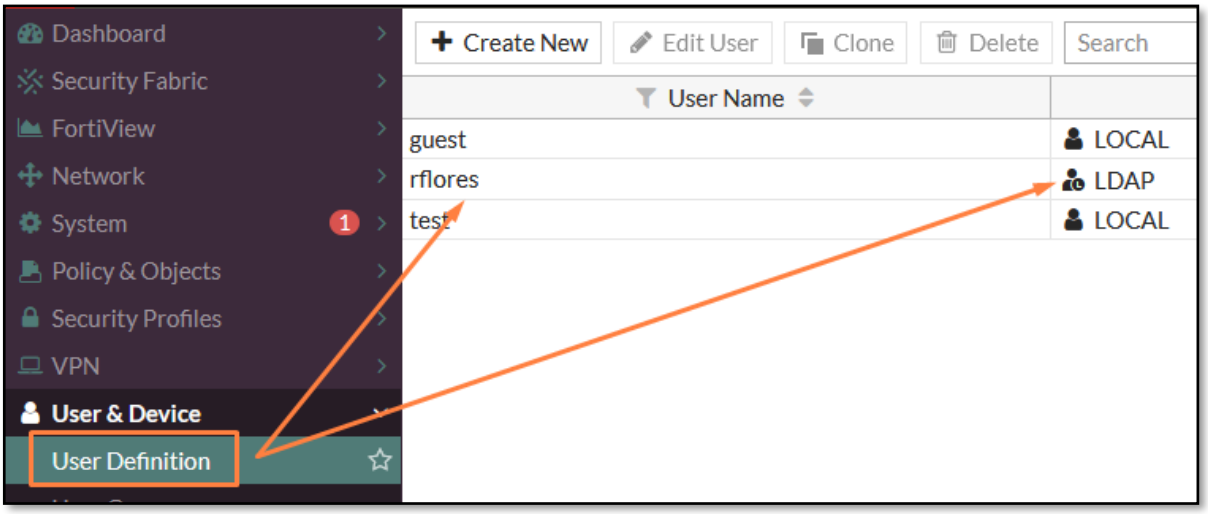


Figura 56. Usuario LDAP declarado en el Firewall

PASO 5: A continuación, editaremos el usuario que declaramos para así asignarle un FortiToken virtual como método de **"Doble Factor de Autenticación"** y un correo para que llegue a la bandeja del usuario un código de activación, tal cual se observa en la imagen como evidencia.

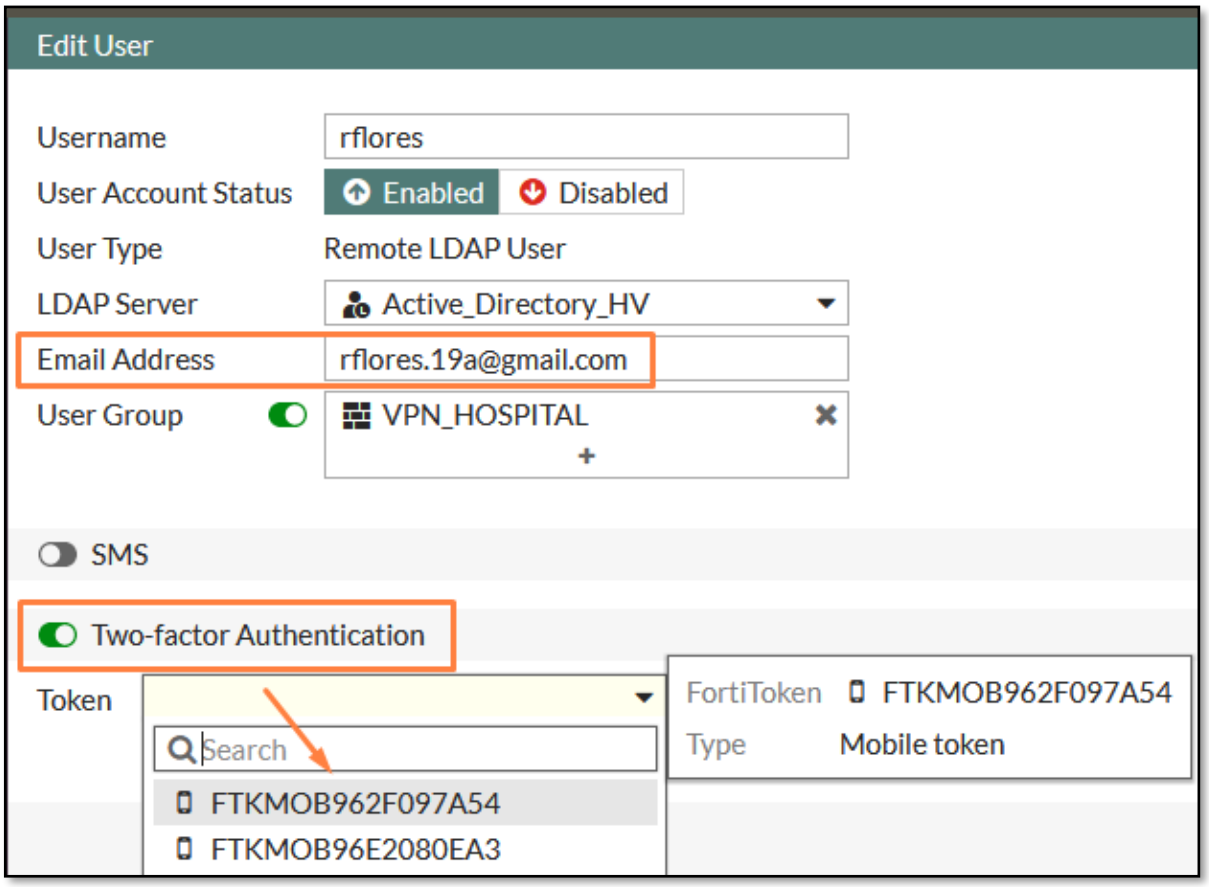


Figura 57. Asignando FortiToken y correo al usuario VPN

PASO 6: Una vez seleccionado el FortiToken podremos observar un mensaje el cual indica que el código de activación ha sido enviado a la bandeja de ese correo.

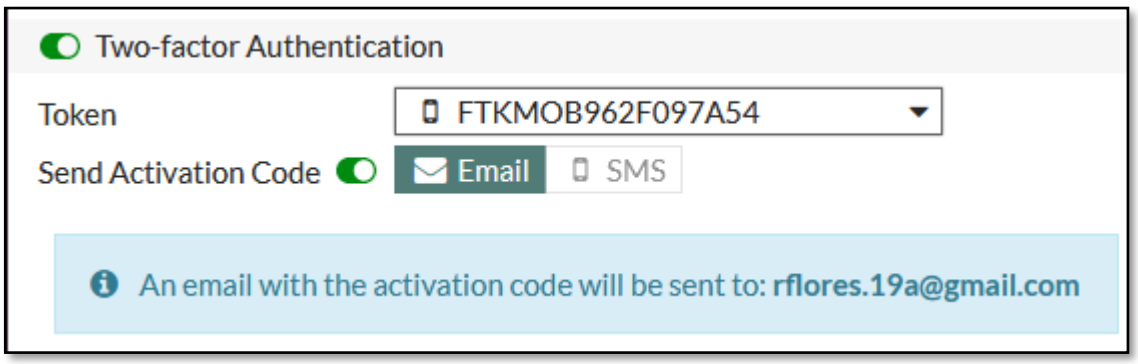


Figura 58. Envío de código de activación al correo personal

PASO 7: Al ingresar al correo personal, podremos verificar que nos llegó un **código de activación** y a la vez un **código QR adjunto**, los cuales podremos utilizarlos para registrar en nuestro aplicativo móvil descargado e instalado.

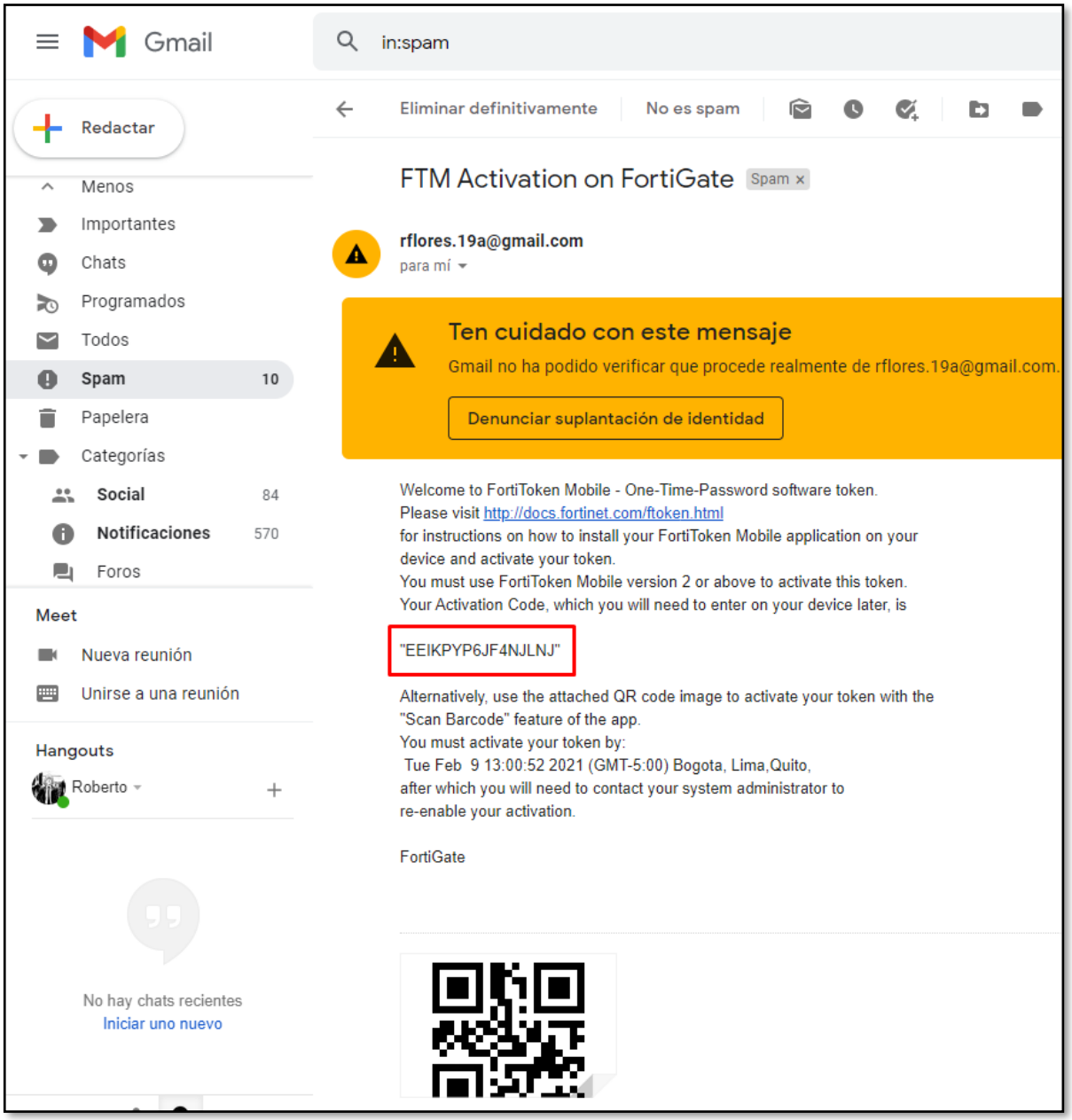


Figura 59. Correo con el código de activación y código QR

PASO 8: Descargamos la aplicación desde el Play Store de nuestro dispositivo móvil que esta disponible y gratuito con el nombre de **"FortiToken Mobile"**

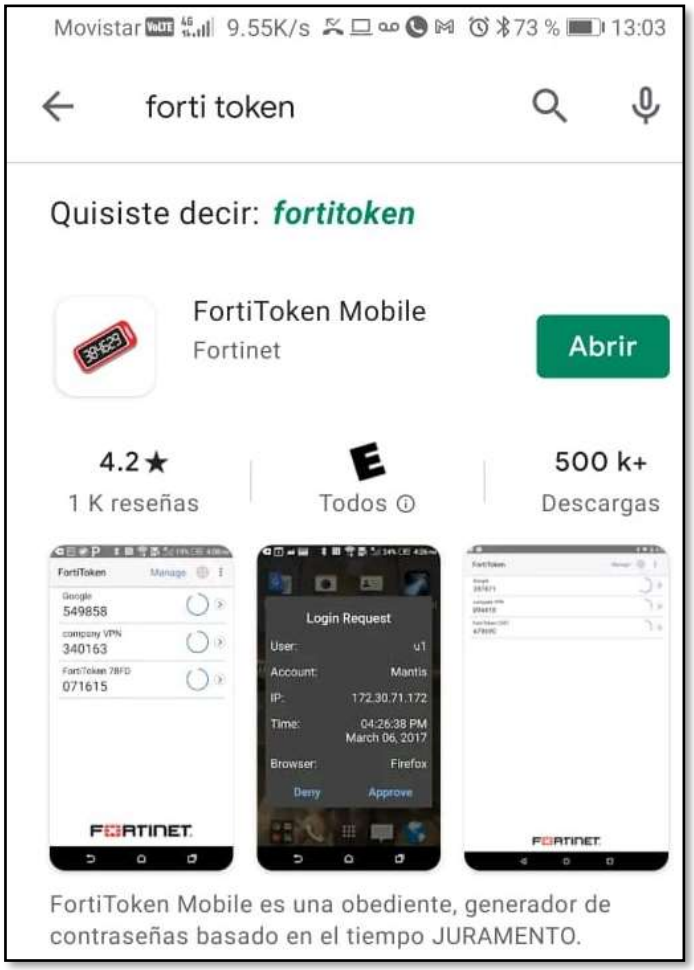


Figura 60. Descarga e instalación del aplicativo FortiToken Mobile

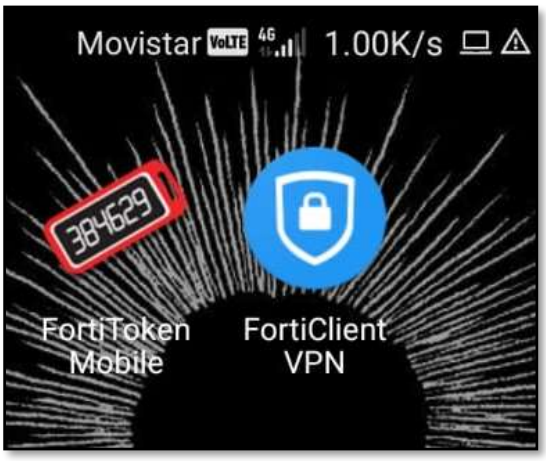


Figura 61. FortiToken Mobile instalado en dispositivo móvil

PASO 9: Al ingresar a la aplicación, seleccionaremos la opción **"SCAN BARCODE"** de la parte inferior, la cual nos ayudará a leer el código QR y automáticamente el FortiToken se sincronice y registre al dispositivo móvil.

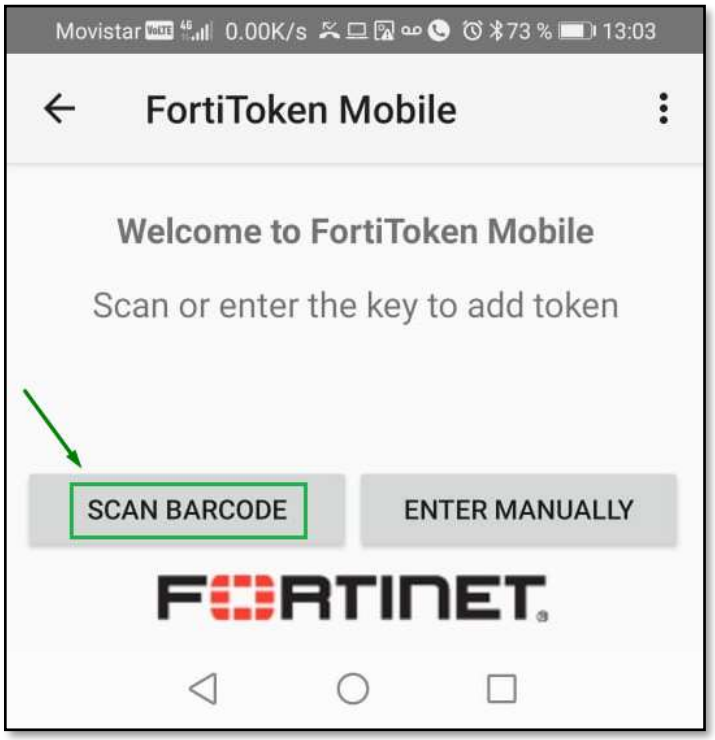


Figura 62. Opciones de registro del FortiToken Mobile

PASO 10: Ahora, veremos que el FortiToken virtual asignado en el Firewall para el usuario "rflores" es el que se registra en el aplicativo "FortiToken Mobile"

Figura 63. FortiToken asociado como doble factor de autenticación

PASO 11: Finalmente, podremos observar que el aplicativo FortiToken Mobile nos asigna un código de 6 dígitos de forma aleatoria a cada minuto, podemos mostrar u ocultar ese código.

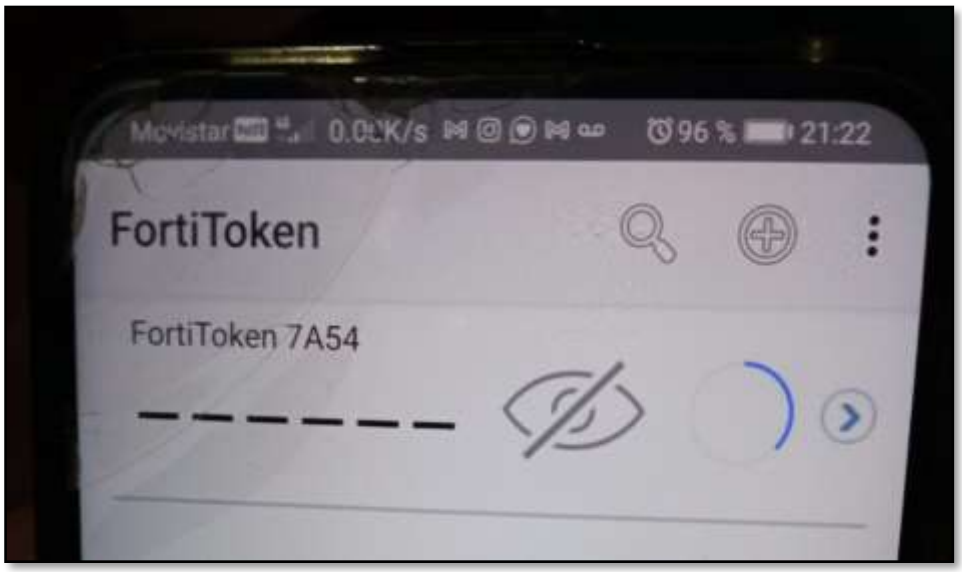


Figura 64. FortiToken con código oculto

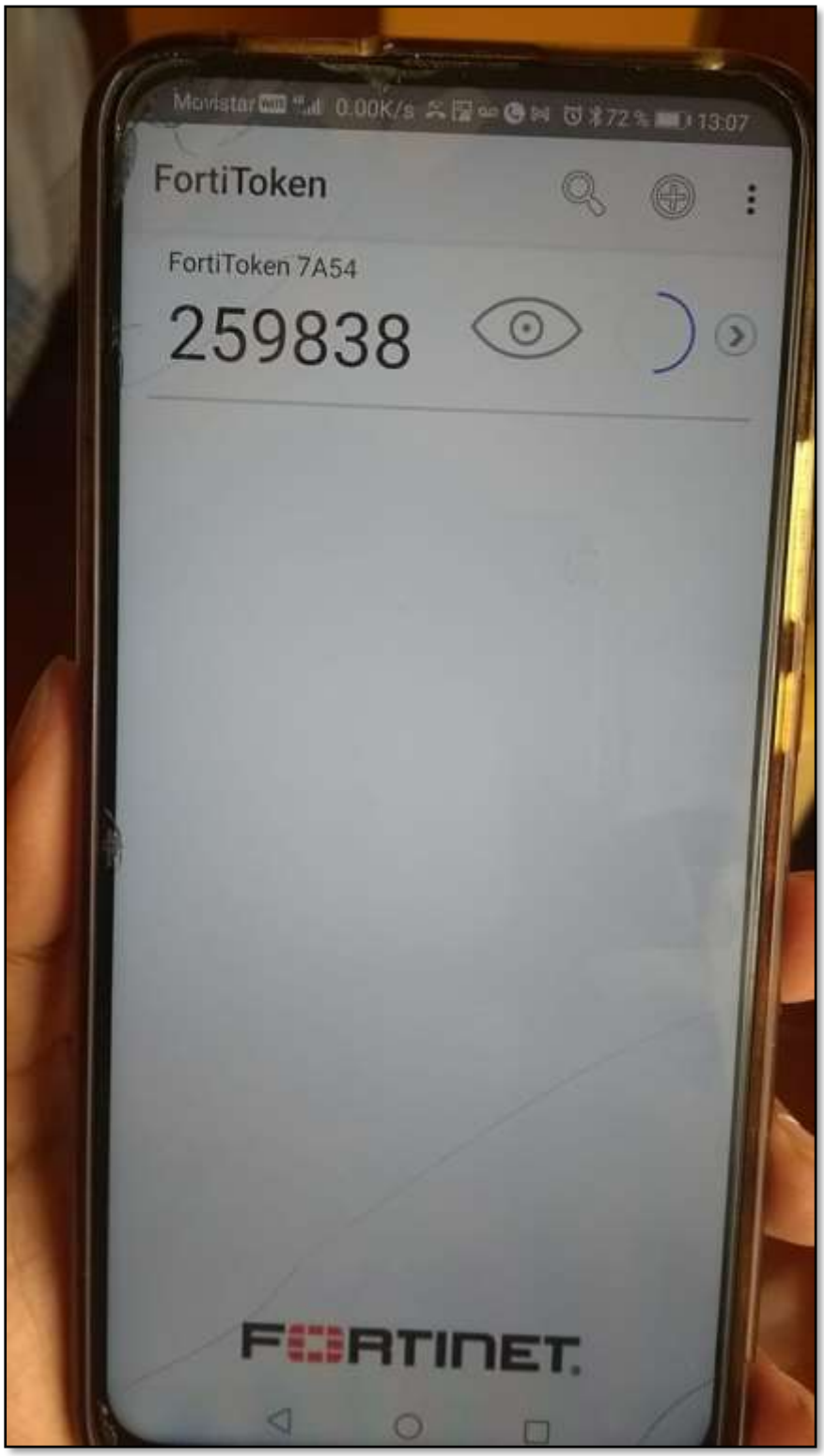


Figura 65. FortiToken generando código

Prueba piloto de la conexión VPN-SSL con método de Doble Factor de Autenticación

PASO 1: Para esta prueba de conexión abrimos el aplicativo FortiClient

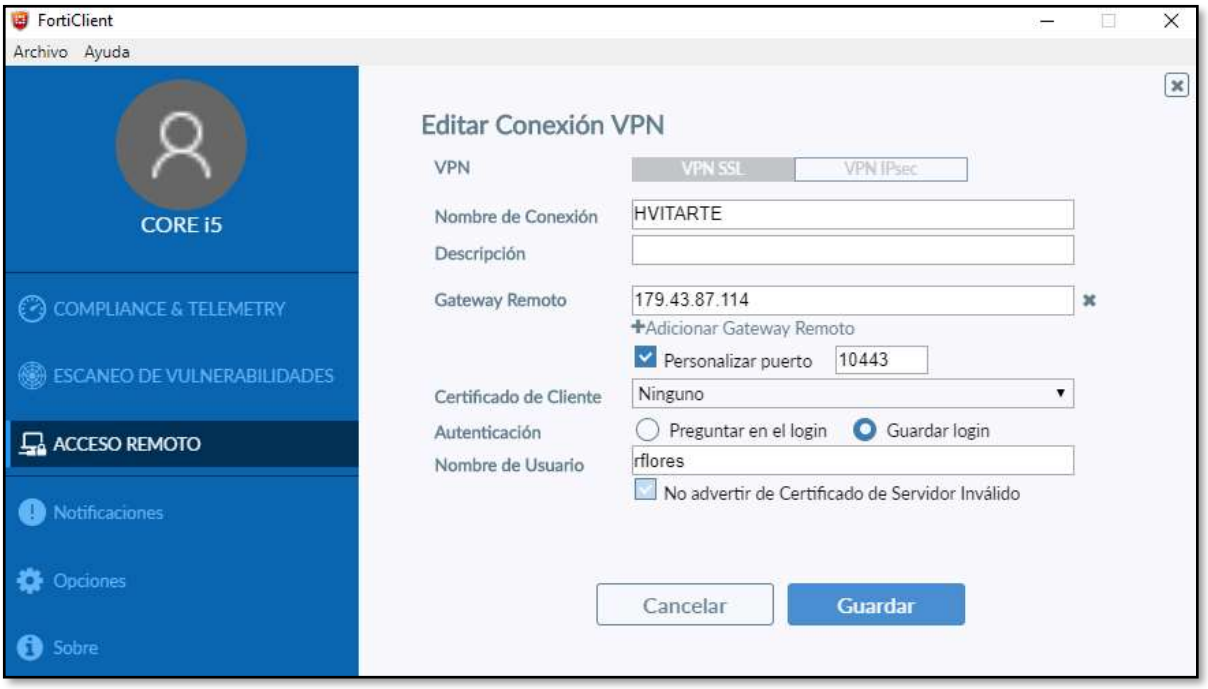


Figura 66. Abriendo el aplicativo FortiClient

PASO 2: Ingresaremos nuestras credenciales VPN y esperamos el estado de carga de conexión del aplicativo.

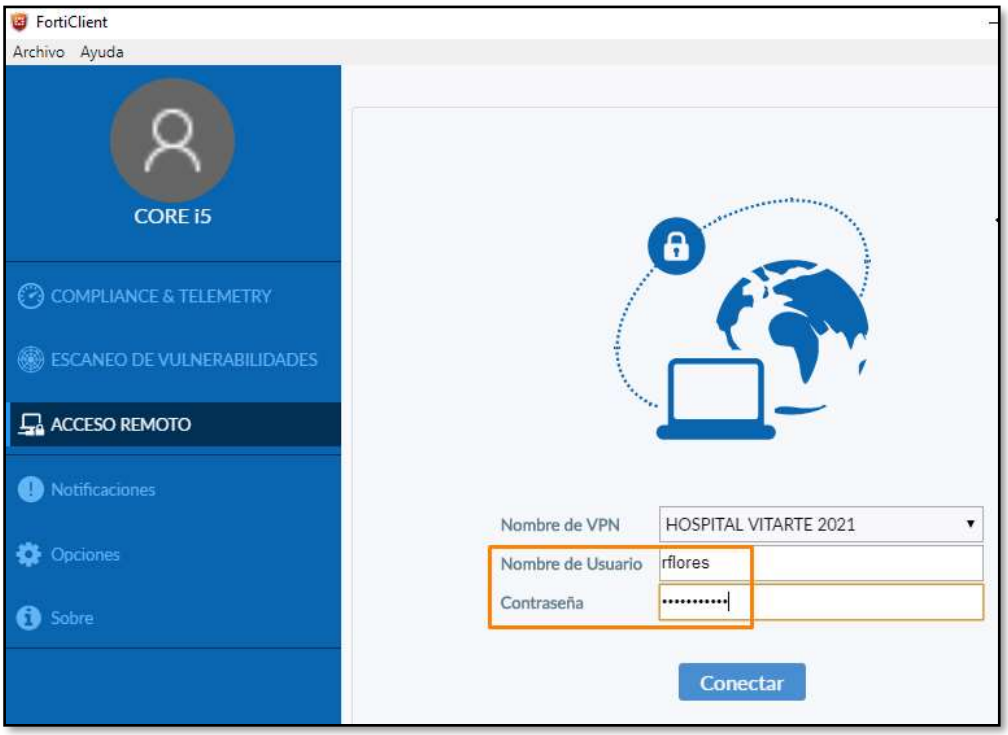


Figura 67. Ingresando credenciales VPN

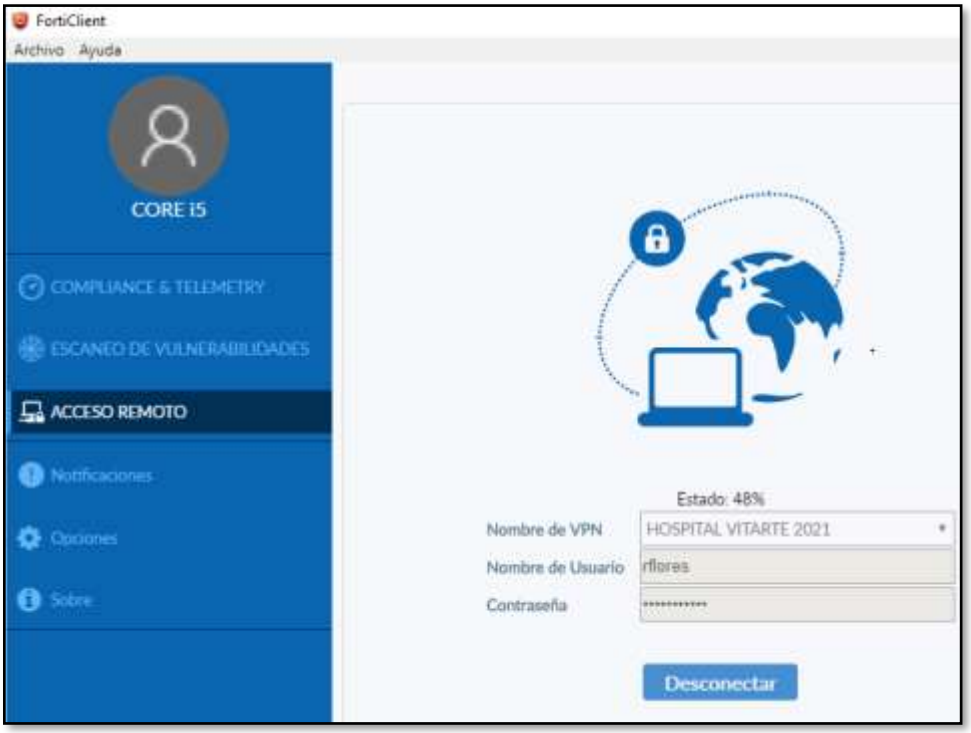


Figura 68. Estado de carga para conexión VPN

PASO 3: Ingresaremos el código que nos genera nuestro aplicativo FortiToken Mobile previamente instalado y configurado en nuestro dispositivo móvil.

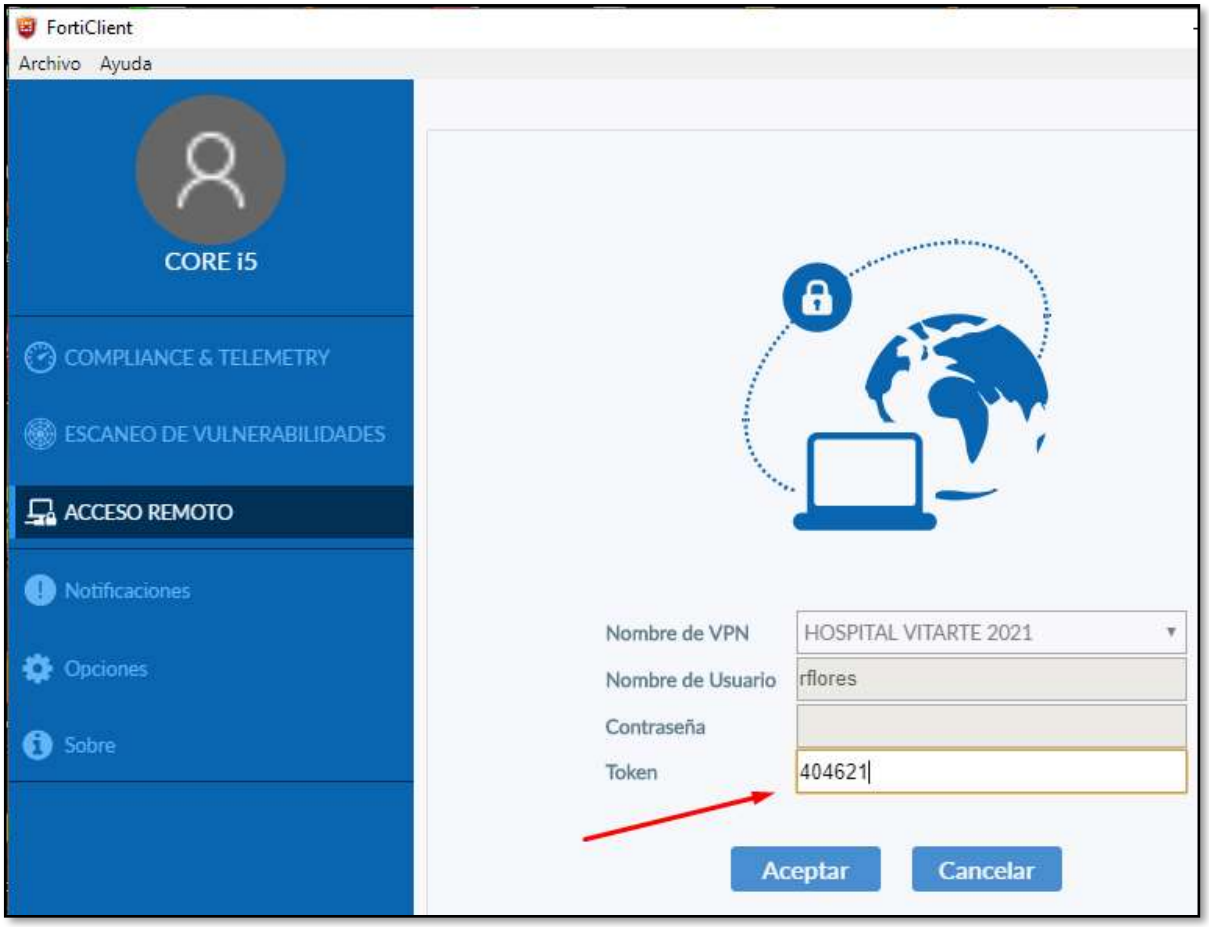


Figura 69. Solicitud de código Token para conexión VPN

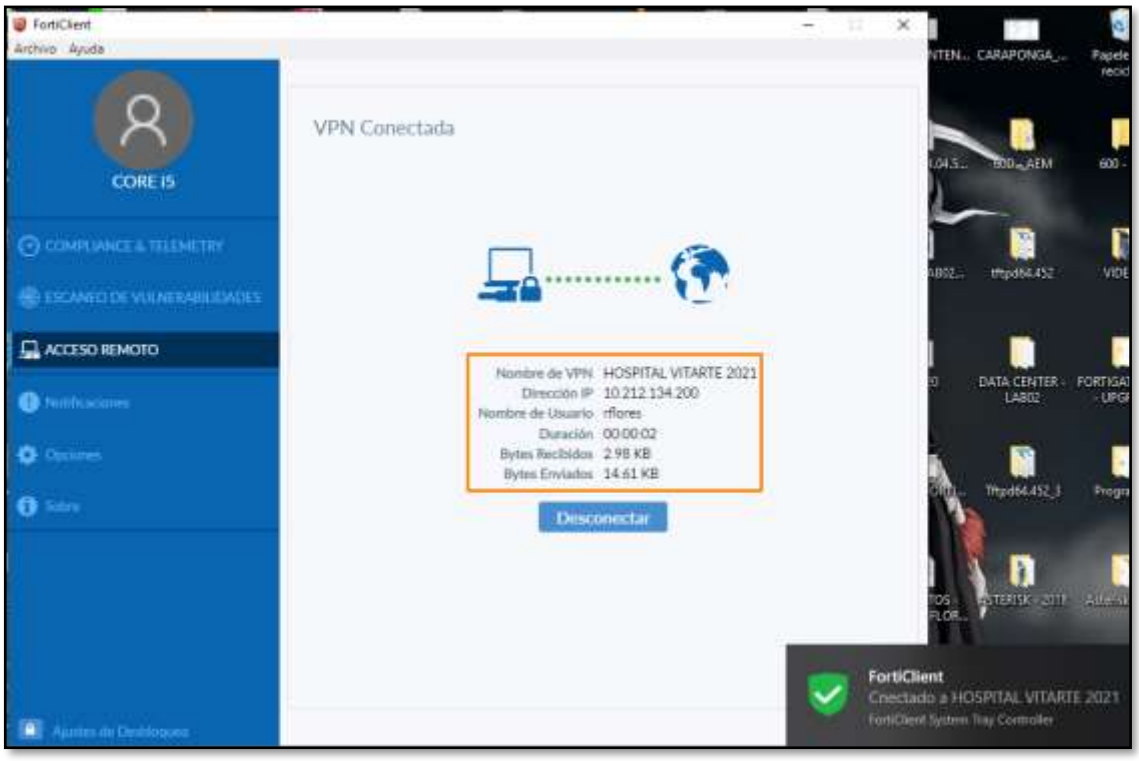


Figura 70. Conexión exitosa de usuario VPN

PASO 4: Ahora podemos ya conectarnos a los sistemas de la red del Hospital de Vitarte.

Figura 71. Conexión RDP a servidor SIGA del HV

3.4.ETAPA DE OPERACIÓN Y CONTROL

Instalación y configuración del aplicativo FortiClient

PASO 1: Primero, descargaremos el FORTICLIENT, aplicativo cliente para la conexión VPN el cual es gratuito y se encuentra en la página web oficial:

https://www.forticlient.com/downloads

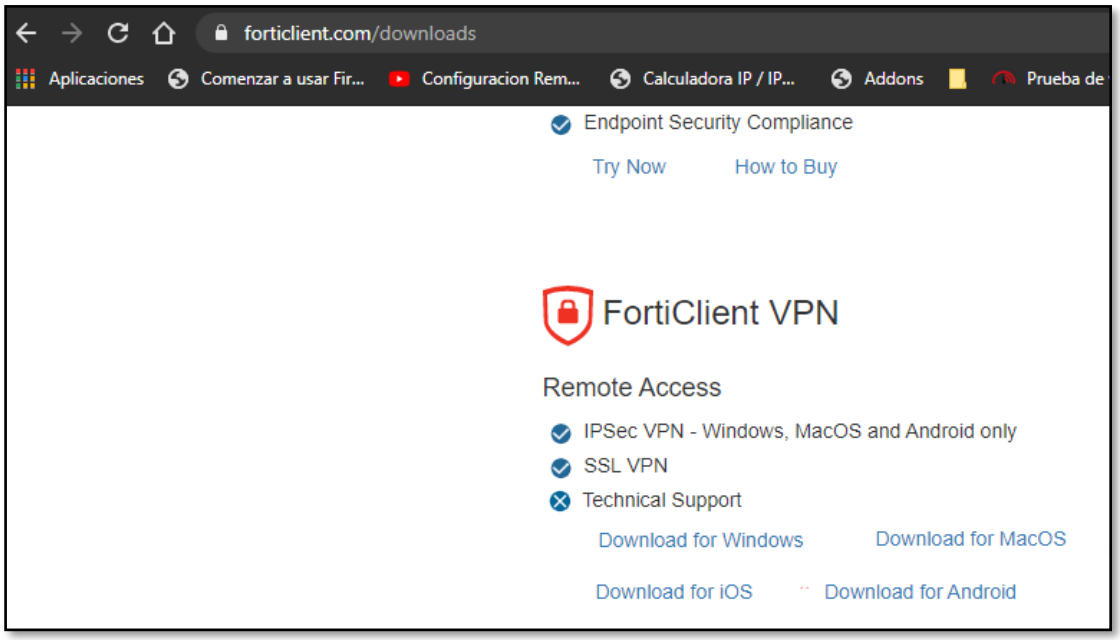


Figura 72. Descarga del FortiClient VPN para Windows

PASO 2: Realizamos doble click en el ejecutable, para empezar a instalar el FortiClient

Figura 73. Descarga del FortiClient VPN para Windows

PASO 3: Activamos la casilla para aceptar el acuerdo de licenciamiento y hacer click en "Next"

Figura 74. FortiClient Setup – Aceptando términos de licencia

PASO 4: Realizar click en el botón "Next" confirmando la ruta de instalación por defecto

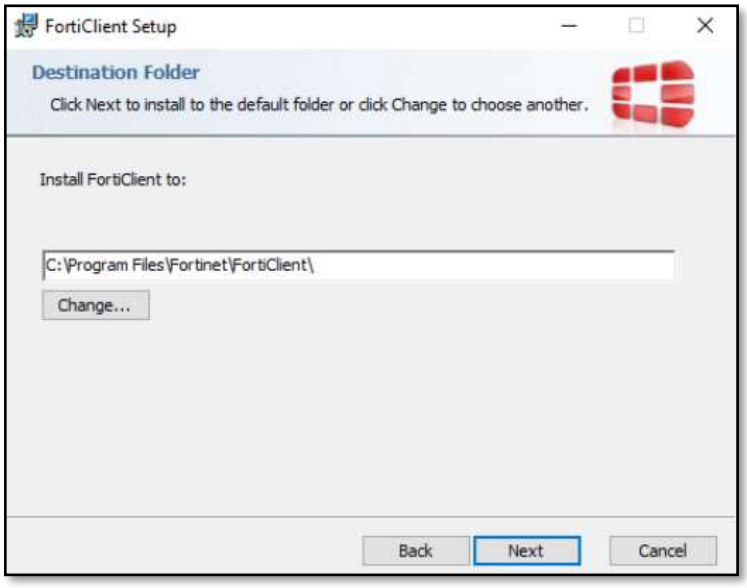


Figura 75. FortiClient Setup – Ruta de instalación

PASO 5: El aplicativo FortiClient comenzará el proceso de instalación

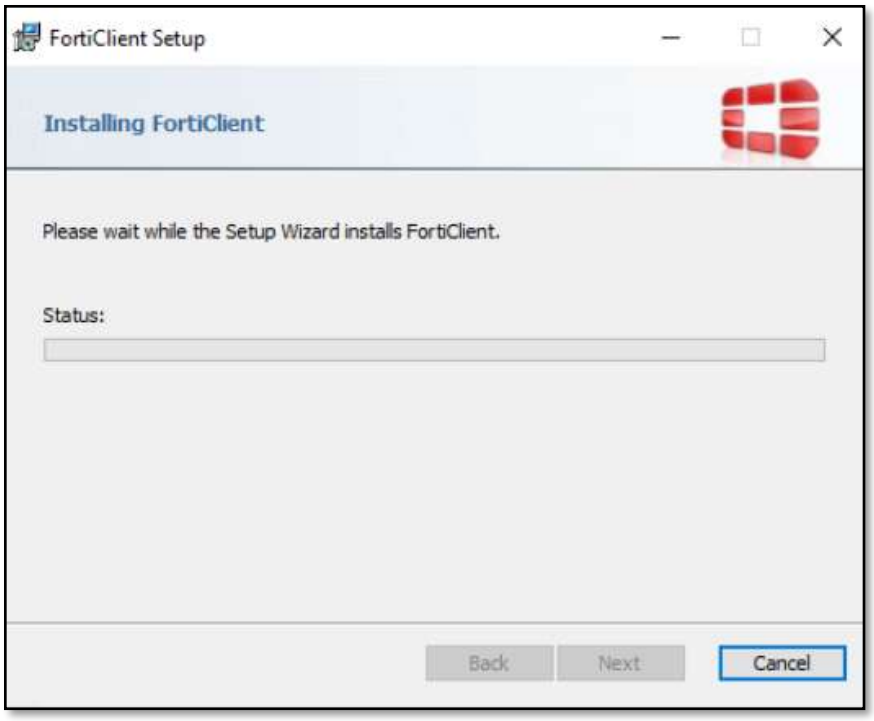


Figura 76. Proceso de instalación del FortiClient

PASO 6: Al culminar la instalación se presentará la siguiente ventana.

Figura 77. FortiClient completamente instalado

PASO 7: Nos dirigimos a la opción "Acceso Remoto" y agregamos los siguientes parámetros:

1. Seleccionar la opción "VPN SSL".
2. Colocar el nombre de conexión: "HOSPITAL VITARTE".
3. En "Descripción" es opcional
4. Colocar en la opción de "Gateway Remoto" la dirección IP: "179.43.87.114".
5. Habilitar la casilla de verificación de: "Personalizar puerto" y a su vez escribir el puerto: "10443".
6. En la opción de "Autenticación" elegir "Preguntar el login".
7. Habilitar la casilla de verificación de: "No advertir de Certificado de Servidor Inválido".
8. Para guardar la configuración realizada dar clic en el botón "Guardar".

Figura 78. Parámetros para la conexión VPN-SSL

Integración del FortiAnalyzer con el FortiGate

PASO 1: Para esto, ya los DNS y sufijos del dominio deben estar configurados en el FortiGate y en el túnel VPN como se observa en las siguientes imágenes:

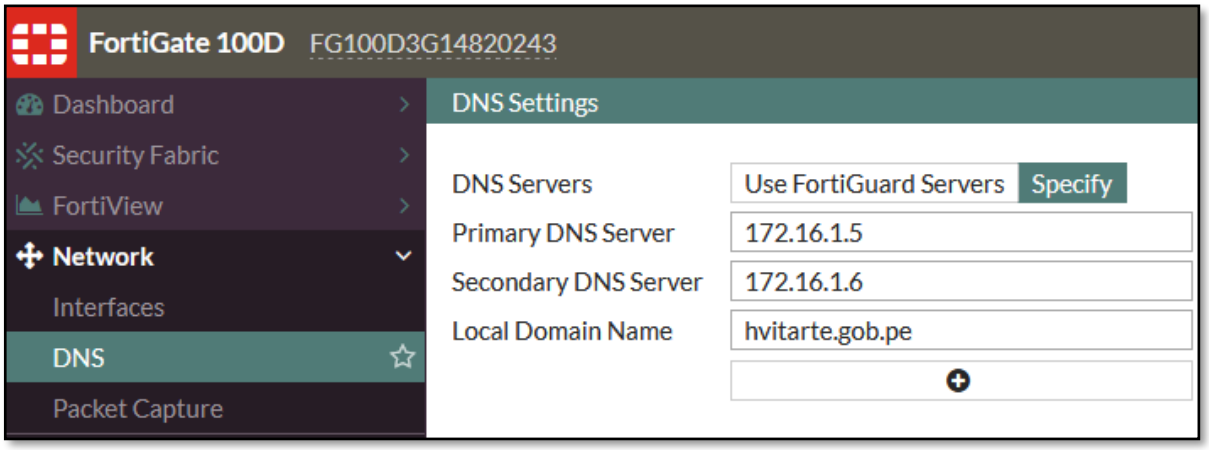


Figura 79. Agregando DNS primario, secundario y sufijo del dominio

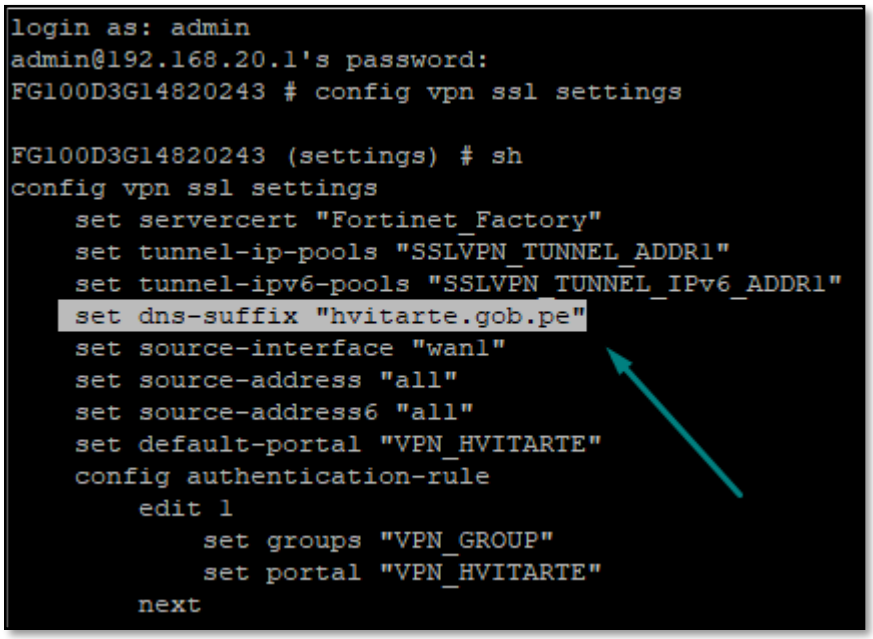


Figura 80. Túnel VPN con el sufijo del dominio agregado

PASO 2: Asignaremos una IP de la red para el FortiAnalyzer y lo registraremos mediante el FortiGate. A continuación, se muestra la ventana principal del FAZ.

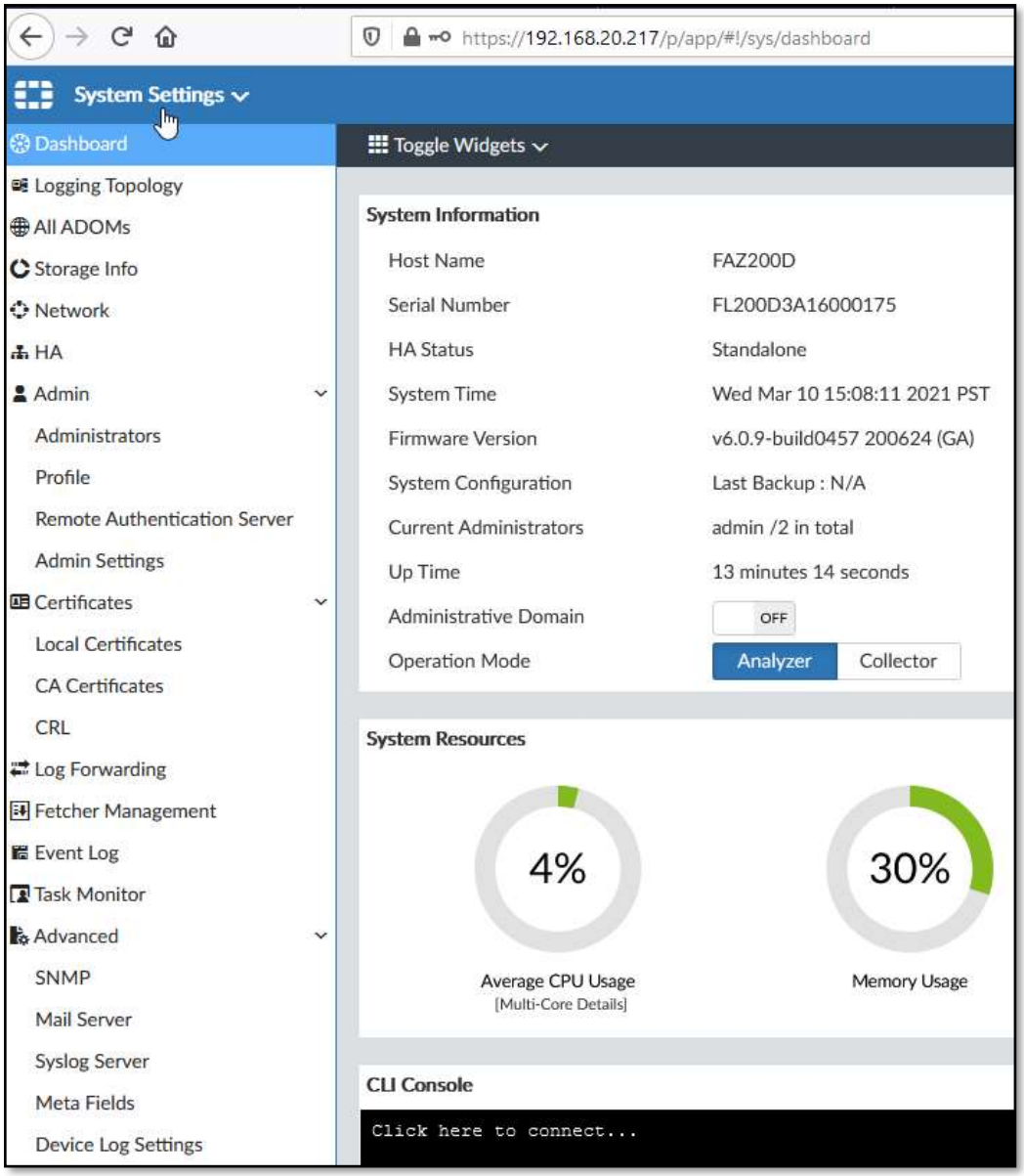


Figura 81. Dashboard inicial del FAZ

PASO 3: Ingresamos al FortiGate y nos dirigimos al apartado **"Log & Report"** en el cual veremos la opción **"Send logs to FortiAnalyzer".**

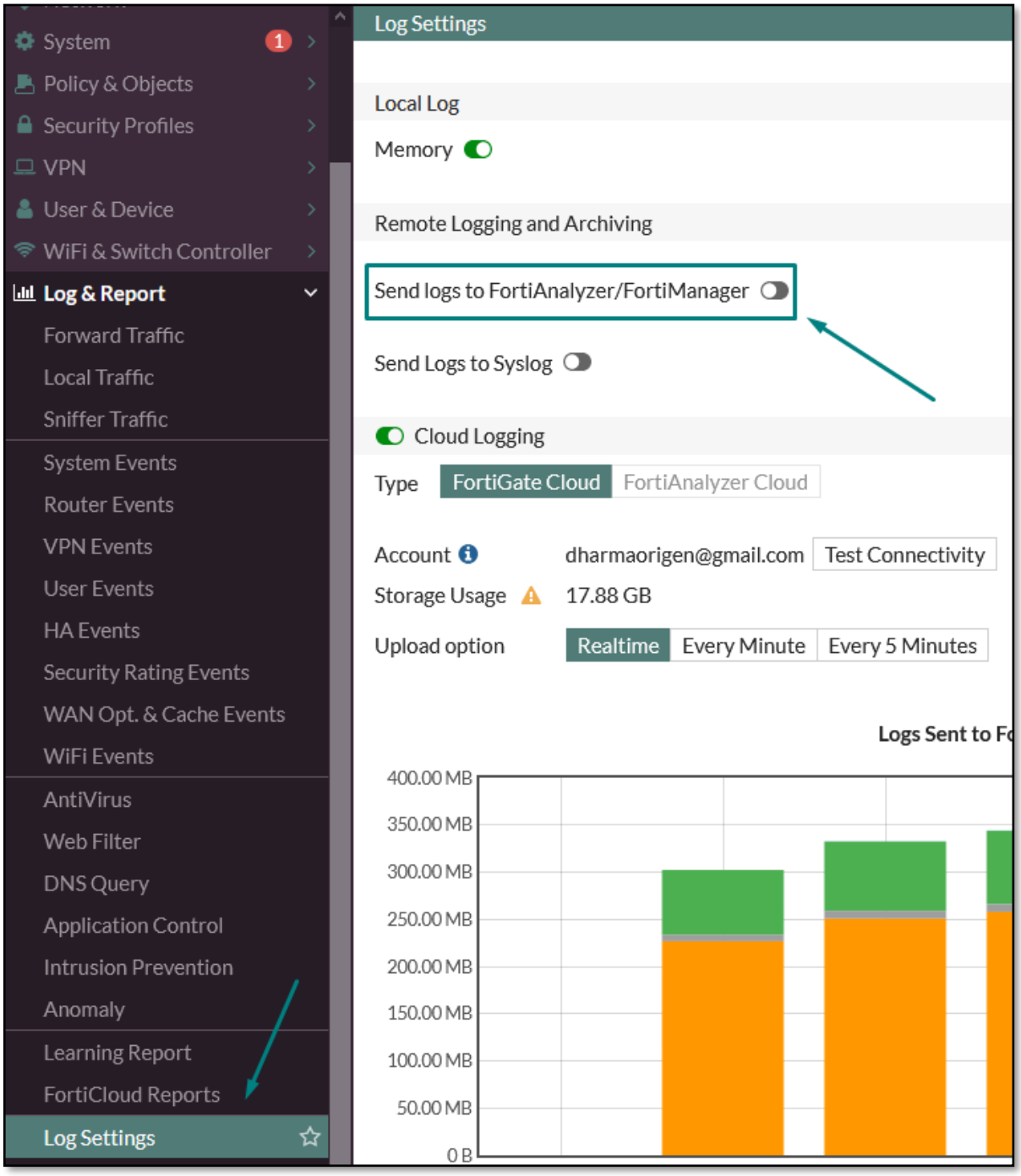


Figura 82. Habilitando el envío de Logs al FAZ

PASO 4: Ingresamos la IP del FortiAnalyzer y seguidamente damos click en **"Test Connectivity"** con esto lograremos que se muestre un mensaje el cual indica que el FortiGate debe ser autorizado por el FortiAnalyzer.

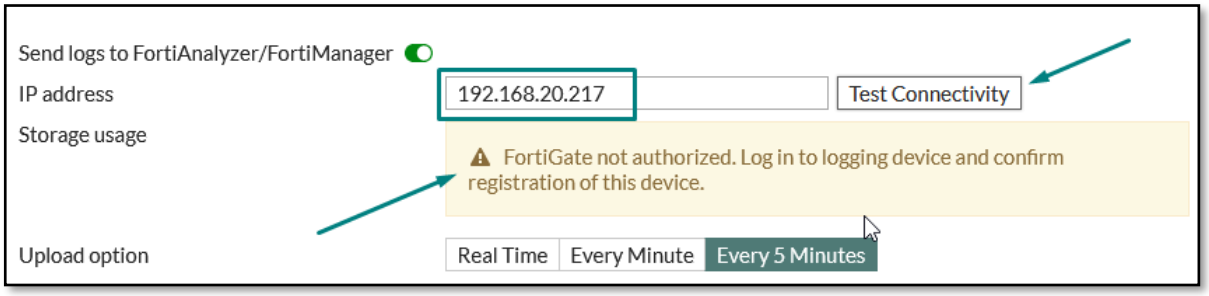


Figura 83. FortiGate no autorizado en el FAZ

PASO 5: Ahora veremos que en el apartado **"Device Manager"** del FortiAnalyzer aparece un equipo aun no registrado.

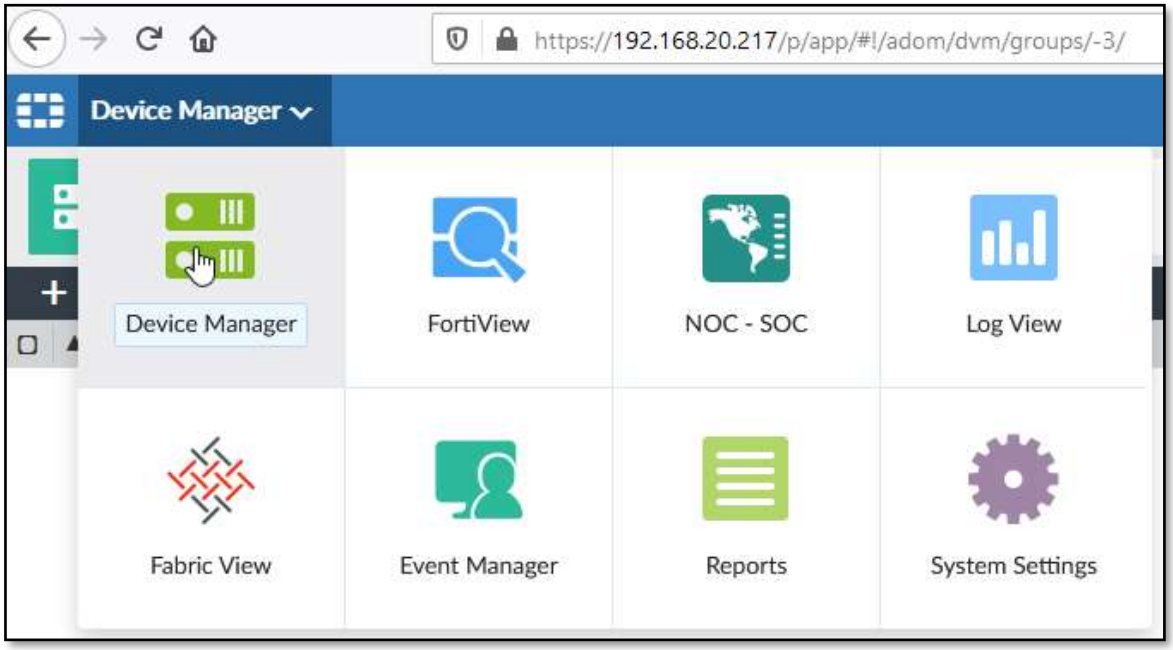


Figura 84. Administración de dispositivos en el FAZ

Figura 85. Device Manager (1 Dispositivo no registrado)

PASO 6: Seleccionamos el FortiGate y lo agregamos para forme parte del FortiAnalyzer.

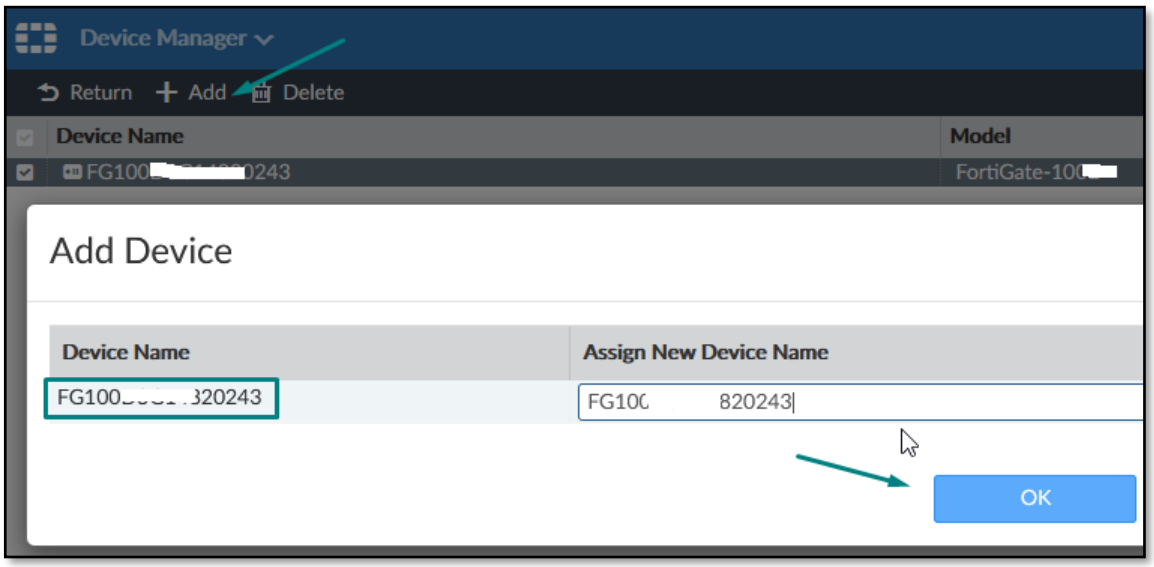


Figura 86. Autorizando y agregando FortiGate al FortiAnalyzer

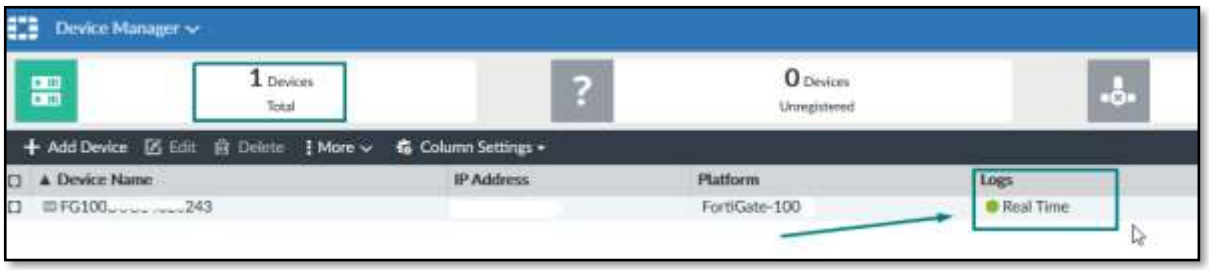


Figura 87. FortiGate autorizado con logs en tiempo real

Monitoreo en tiempo real a través del FortiGate

El monitoreo en tiempo real te lo puede ofrecer el mismo equipo FortiGate en el apartado **"SSL VPN Monitor"** donde nos muestra campos como el usuario conectado, la fecha y hora actual, la IP publica de donde está realizando dicha conexión y la IP asignada por el túnel para el cliente.

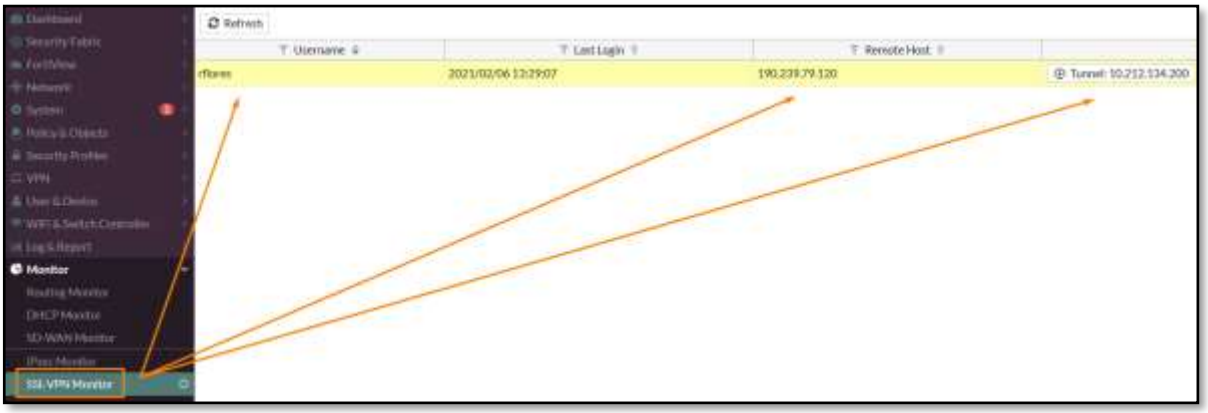


Figura 88. Monitoreo de conexión en tiempo real mediante el FortiGate

Aquí una ampliación de la conexión en tiempo real capturada por el Firewall.

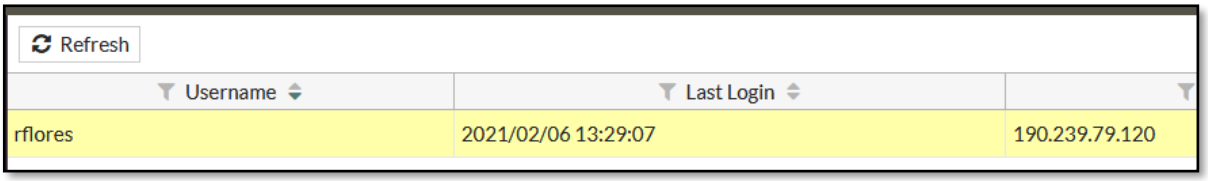


Figura 89. Ampliación de la conexión en tiempo real del usuario remoto

Auditoría de reportes personalizados de conexión en el FortiAnalyzer

Con nuestro FortiAnalyzer sincronizado y configurado anteriormente podremos ingresar al apartado "**Reports"** y veremos múltiples opciones de personalización como predeterminadas.

Entre ellas tenemos las siguientes:

- All Reports (Búsqueda de todos los reportes predeterminados existentes)
- Templates (Plantillas predeterminadas)
- Chart Library (Liberia de códigos y gráficos)
- Datasets (Sentencias SQL y conjunto de datos tabulados)

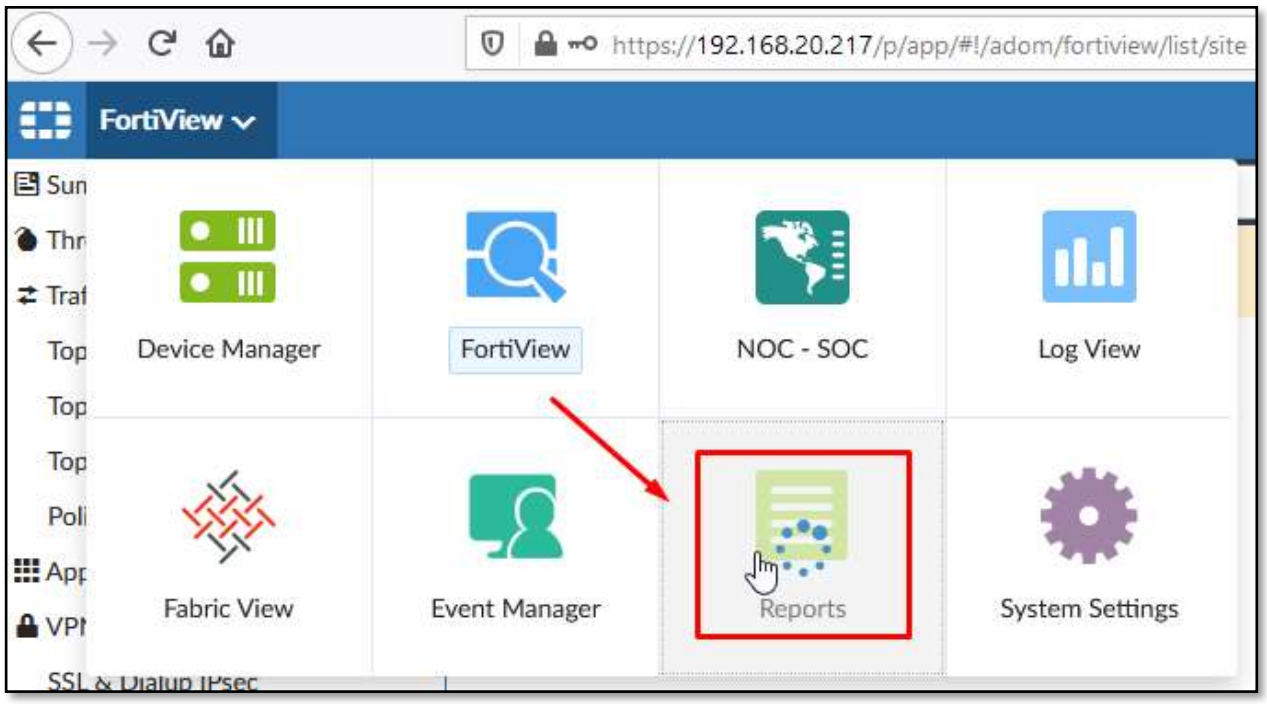


Figura 90. Ingreso a la opción de Reportes en el FortiAnalyzer

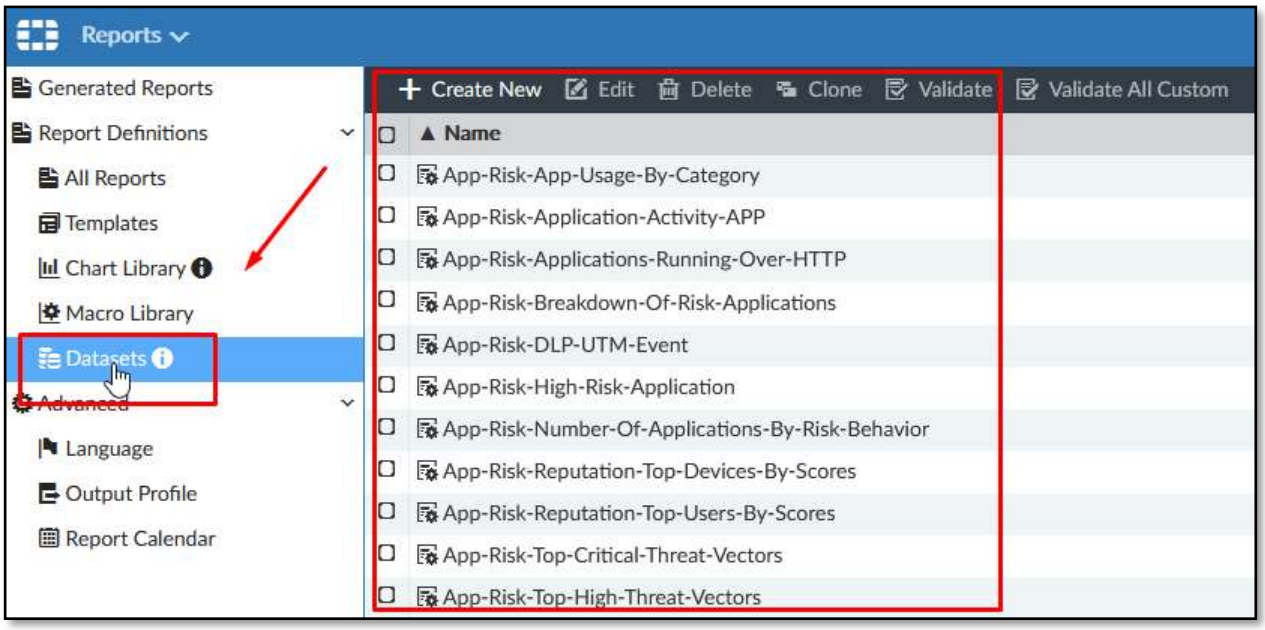


Figura 91. Opciones para crear y personalizar reportes

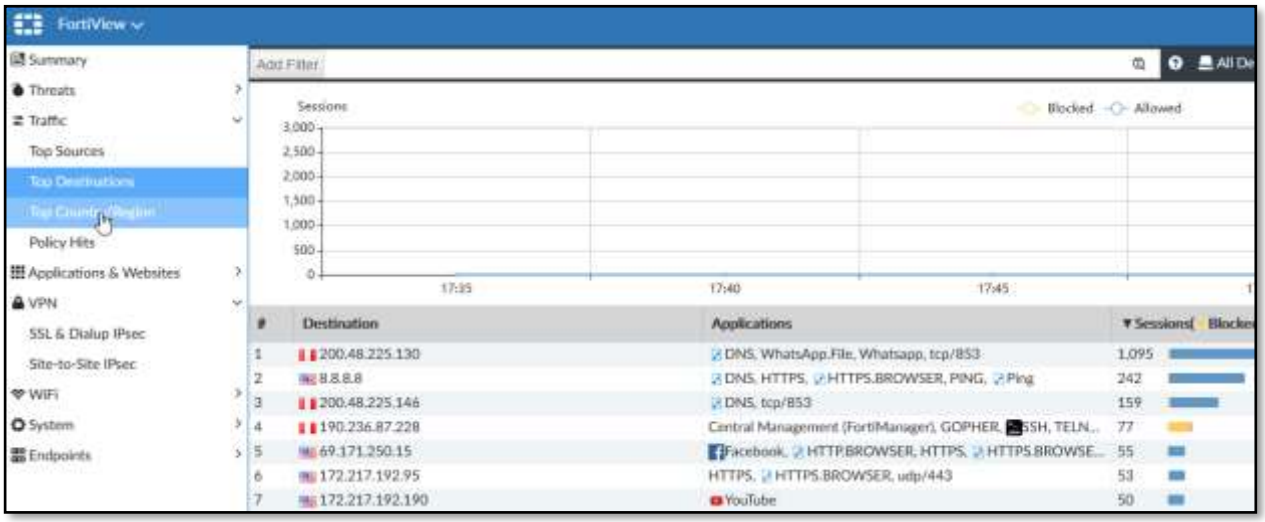


Figura 92. Opciones de visualización en tiempo real de las conexiones

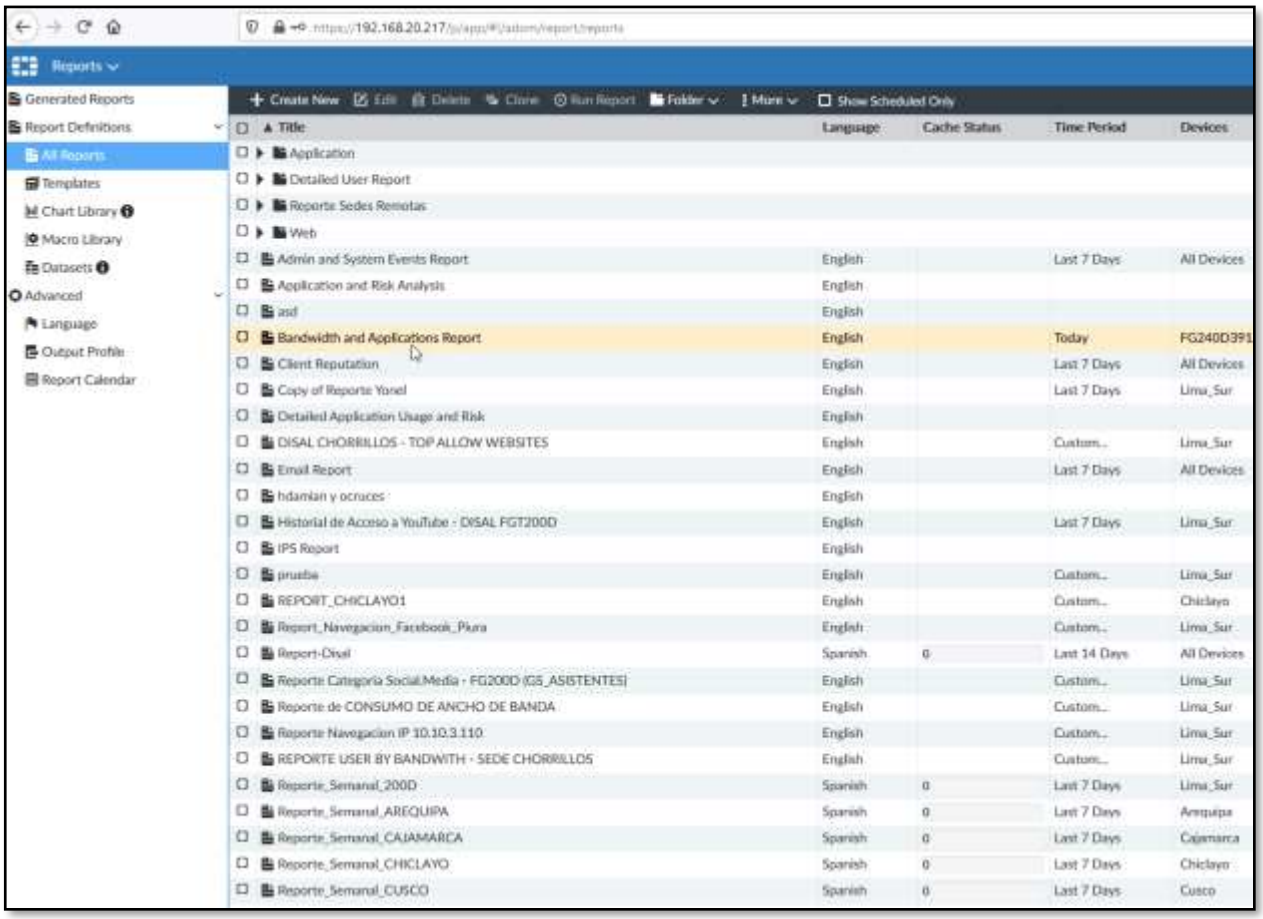


Figura 93. Variedad de reportes personalizados para distintas auditorias

CAPITULO 4

RESULTADOS

4.1.Resultados

4.1.1. PRIMER RESULTADO:

Se logra cumplir el **"Método de doble factor de autenticación"** como acceso legitimo del trabajador remoto mediante la VPN-SSL a través del Firewall FortiGate-100E.

Demostración – Parte 1: Para evidenciar este resultado nos conectamos a una red inalámbrica externa con una laptop para ingresar a la VPN como corresponde.

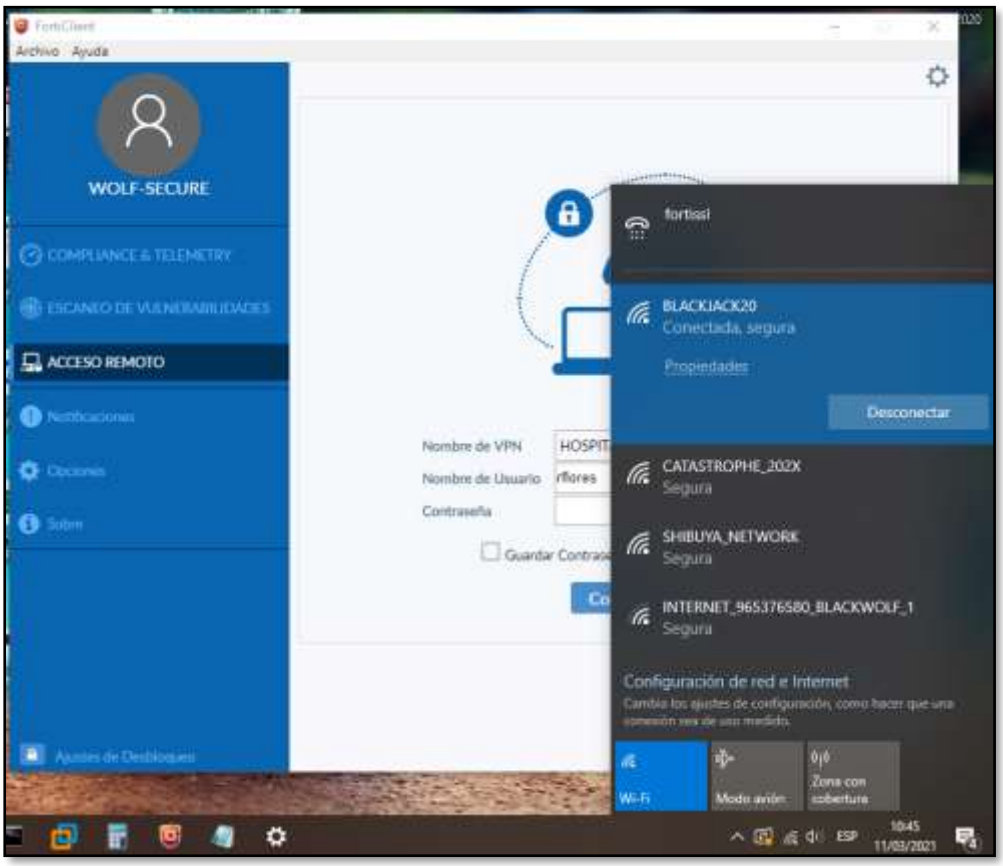


Figura 94. Conexión a red inalámbrica externa desde laptop

Demostración – Parte 2: Como primer método de factor de autenticación **(ALGO QUE SABEMOS)** ingresaremos nuestro usuario del dominio y su respectiva contraseña.

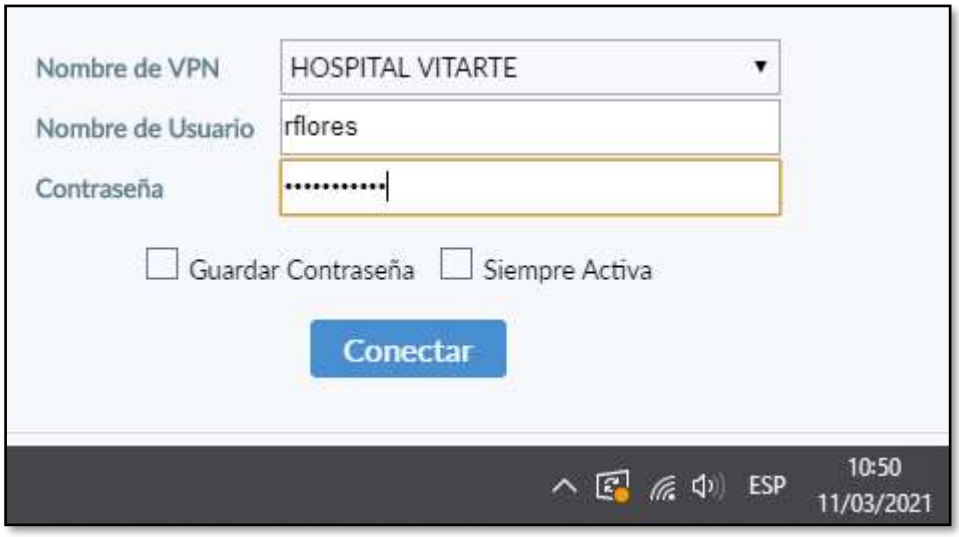


Figura 95. Primer factor de autenticación (Algo que sabemos)

Demostración – Parte 3: Como segundo método de factor de autenticación **(ALGO QUE POSEEMOS)** ingresaremos nuestro código que nos genera nuestro FortiToken Mobile ya registrado en nuestro dispositivo móvil.

Figura 96. Segundo factor de autenticación (Algo que poseemos)

Demostración – Parte 4: De esta manera logramos la conexión a la VPN cumpliendo el **"Método de Doble Factor de Autenticación"**

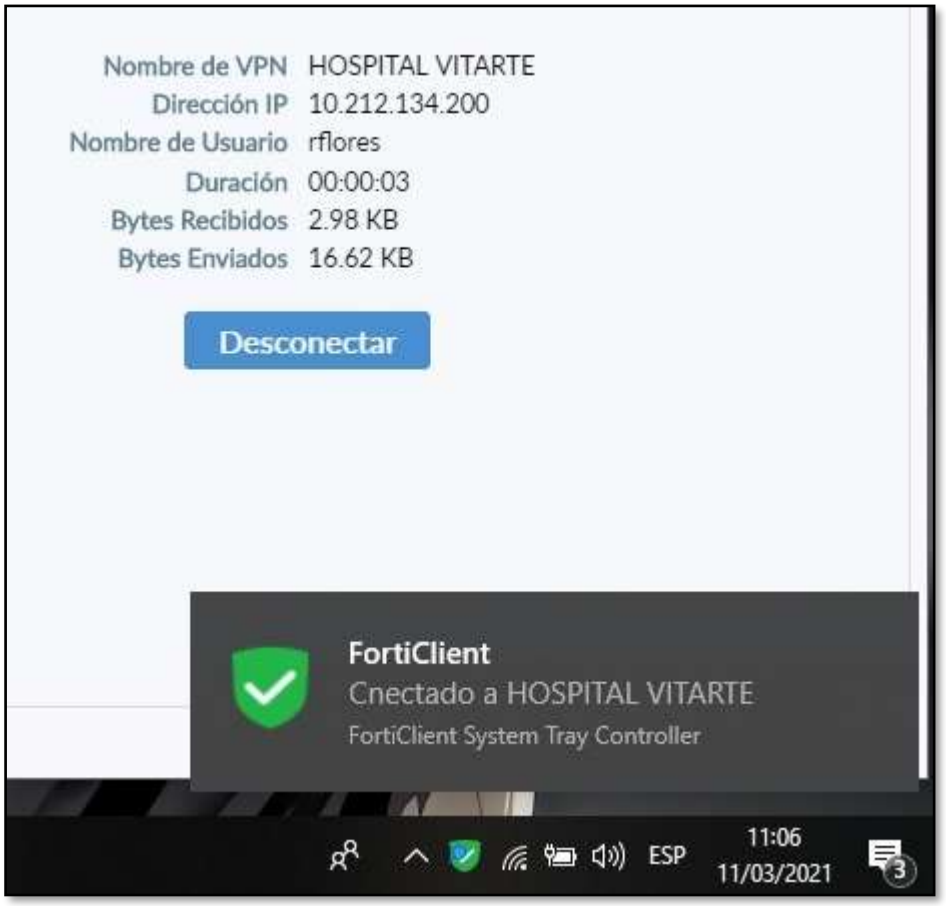


Figura 97. Conexión VPN exitosa cumpliendo el Método de Doble Factor de Autenticación

Incluso aquí evidenciamos todas las licencias FortiToken agregadas y la asignación de cada una de ellas para cada usuario VPN, ahora todos los usuarios tienen el **Doble Factor de Autenticación.**

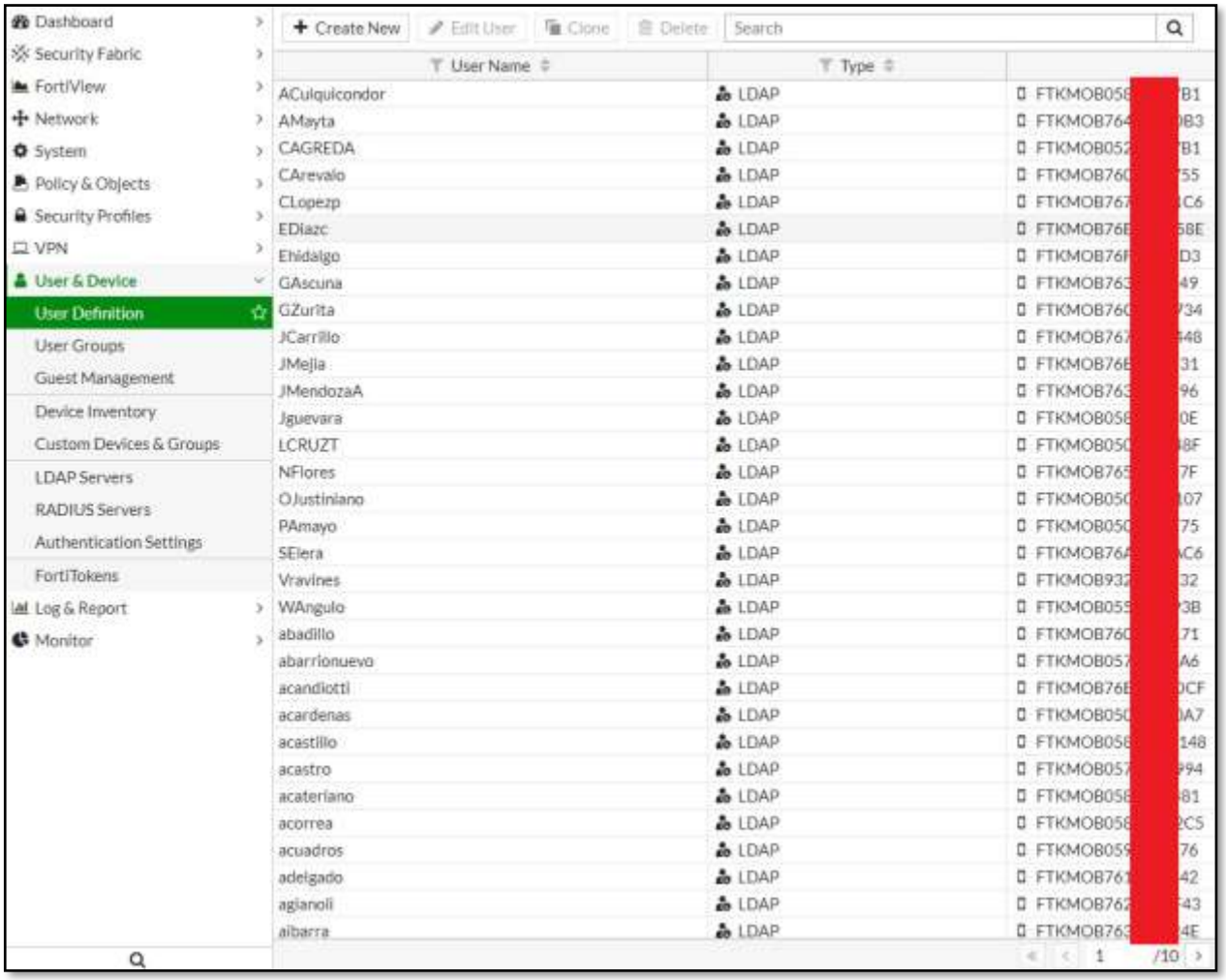


Figura 97-1. Licencias FortiToken registradas y asignadas en el Firewall

Demostración – Parte 5: De la misma manera podemos intentar la conexión mediante nuestro dispositivo móvil mediante el FortiClient el cual está disponible para Android y IOS.

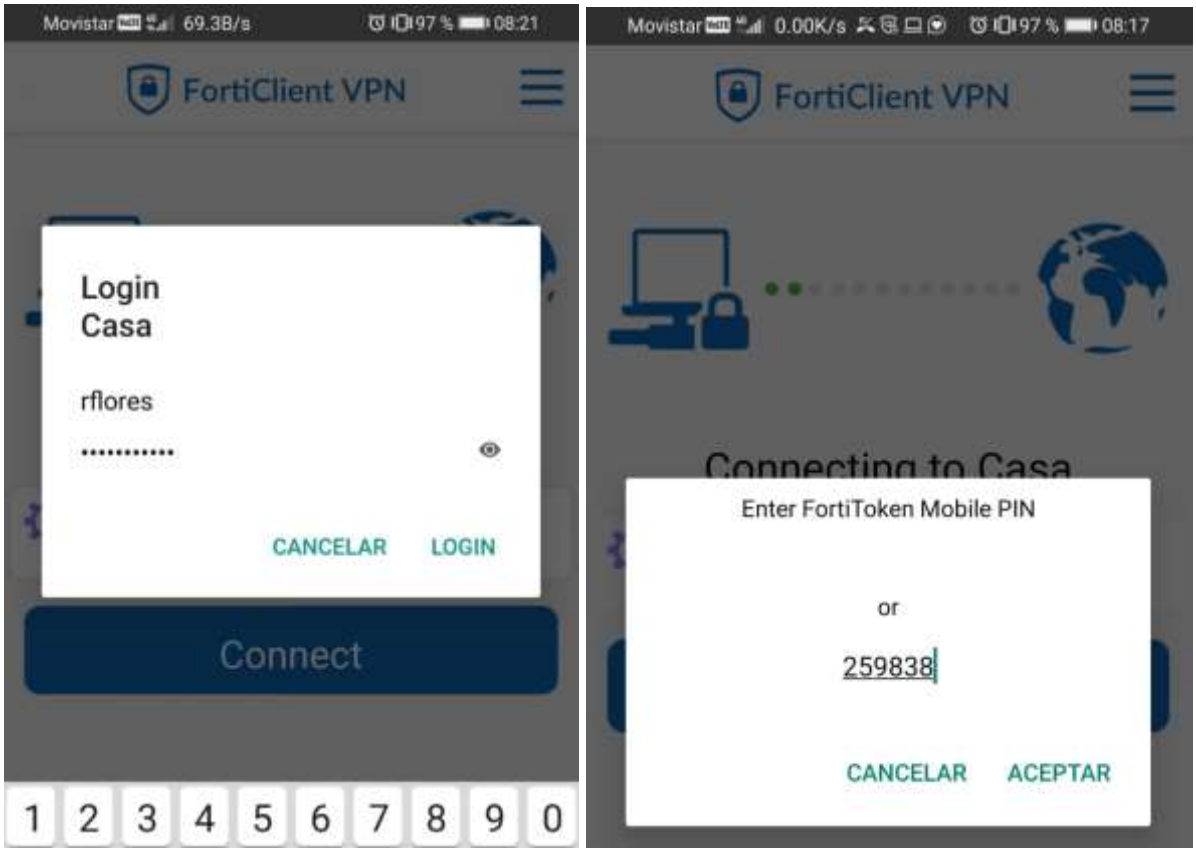


Figura 98. Doble factor de Autenticación a través del aplicativo FortiClient para móvil

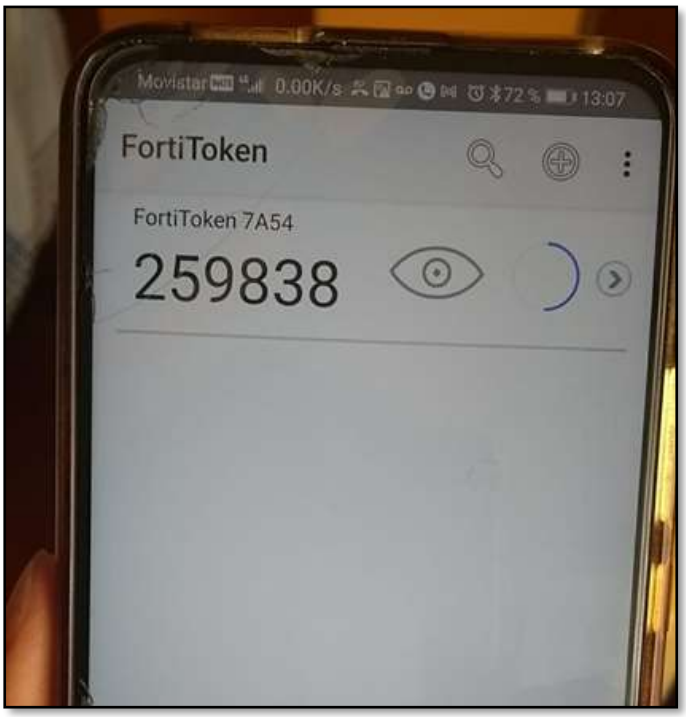


Figura 99. FortiToken registrado en dispositivo móvil

4.1.2. SEGUNDO RESULTADO:

Se consigue ingresar a los sistemas, recursos y aplicaciones alojadas en los servidores del Hospital de Vitarte, cumpliendo así las actividades o roles asignados por cada unidad o servicio en la modalidad de Teletrabajo mediante una VPN-SSL a través del Firewall FortiGate-100E.

Demostración – Parte 1: Ya conectados a la VPN incluso podremos hacer un ping ya sea por IP o por HOSTNAME de los servidores del Hospital de Vitarte como evidencia de que podemos hacer resolución de nombres mediante la VPN.

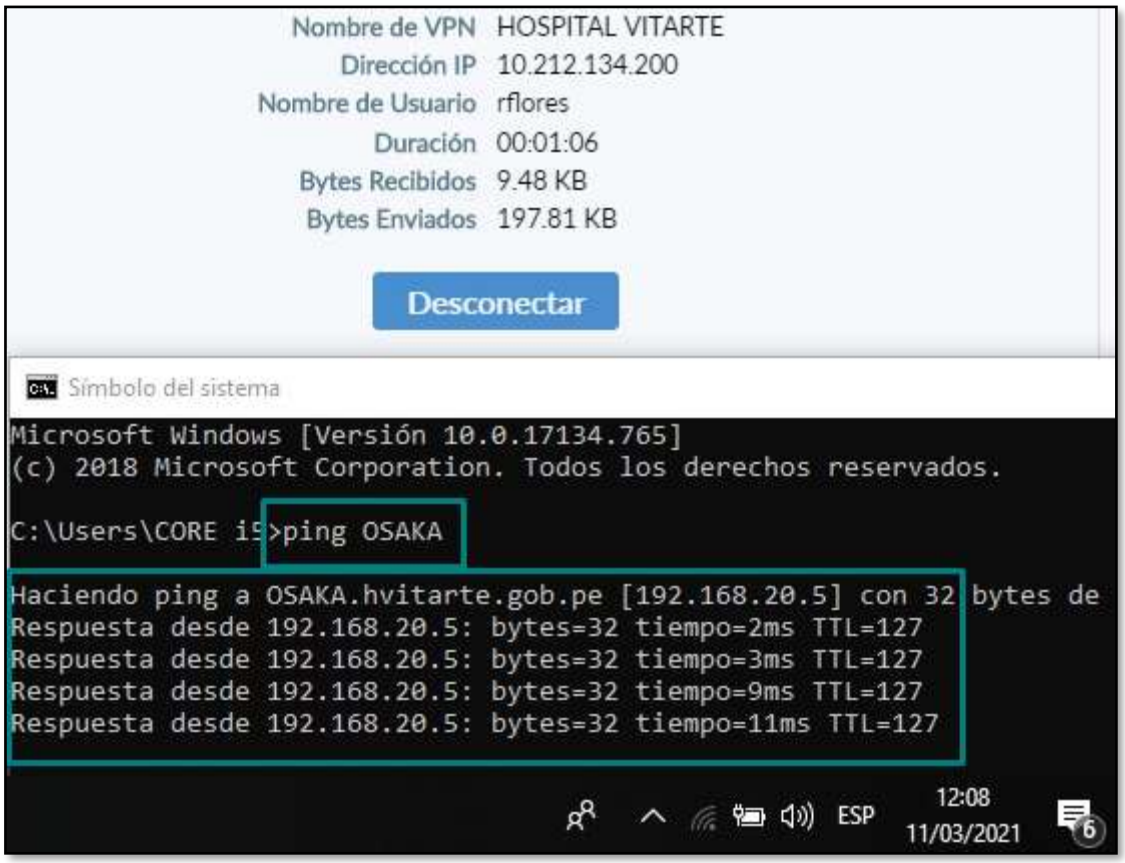


Figura 100. Prueba de conectividad hacia hostname del AD mediante la VPN

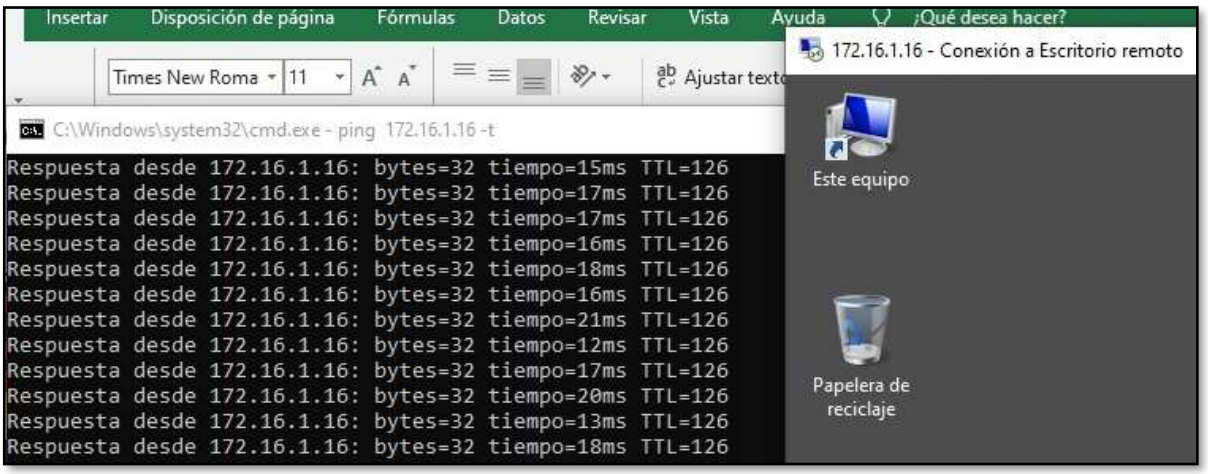


Figura 101. Prueba de conexión ping y RDP

Demostración – Parte 2: De esta manera cualquier equipo cliente conectado a la VPN puede incluso unirse al dominio **HVITARTE** o ejecutar las aplicaciones directamente, comenzar a trabajar y cumplir sus actividades asignadas por su jefatura.

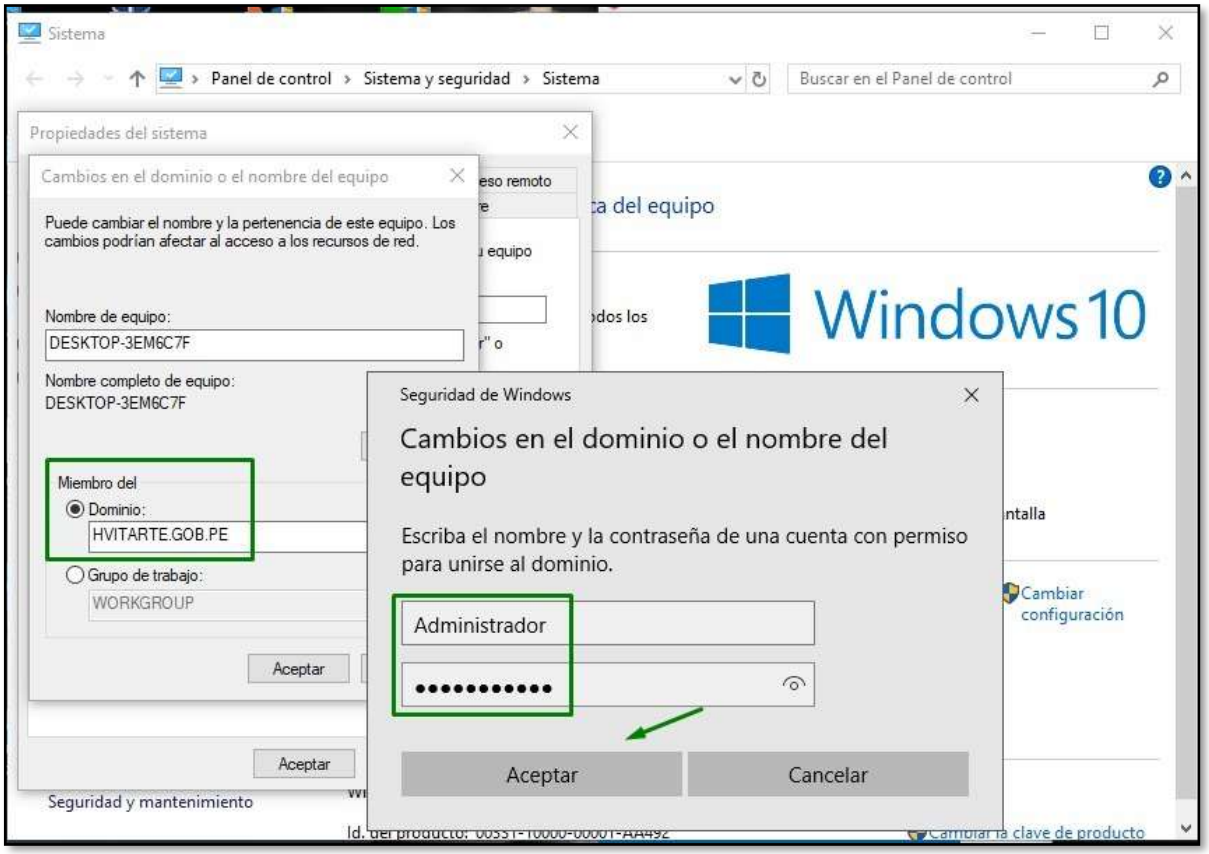


Figura 102. Equipo cliente conectado por la VPN uniéndose al dominio HVITARTE

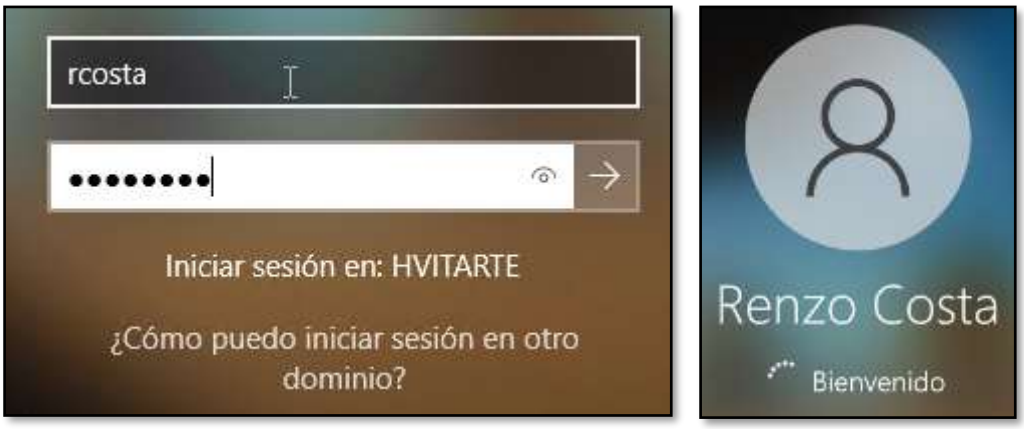


Figura 103. Inicio de sesión del usuario del dominio

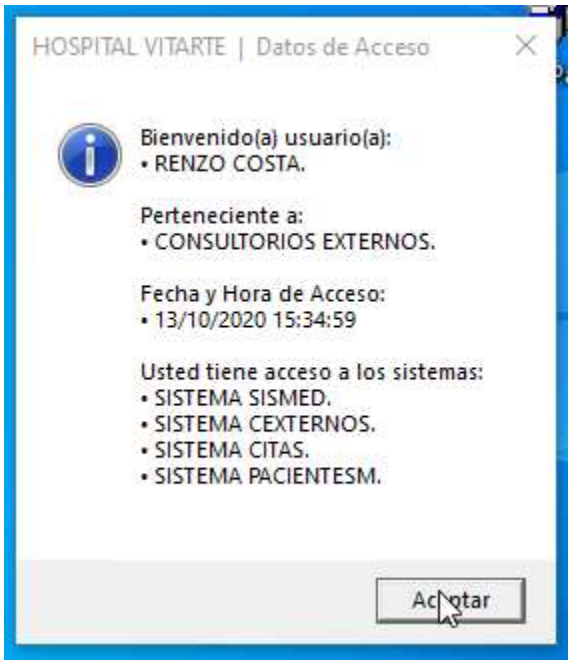


Figura 104. Sistemas mapeados y asignados para el usuario

Demostración – Parte 3: Se evidencia el ingreso a los distintos sistemas y aplicaciones propias del Hospital de Vitarte y la carga de sistemas que son previamente amarrados para cada usuario del dominio según unidad o área a la cual pertenezca.

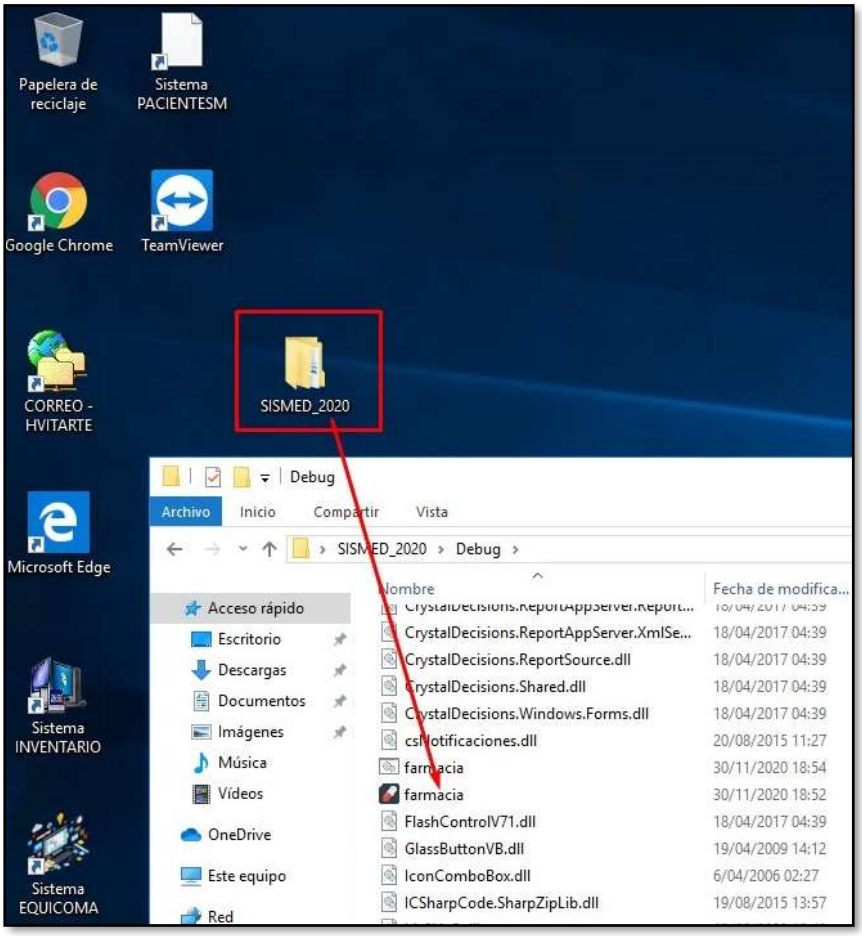


Figura 105. Conexión directa al sistema de Farmacia

Figura 106. Login para el sistema de Farmacia

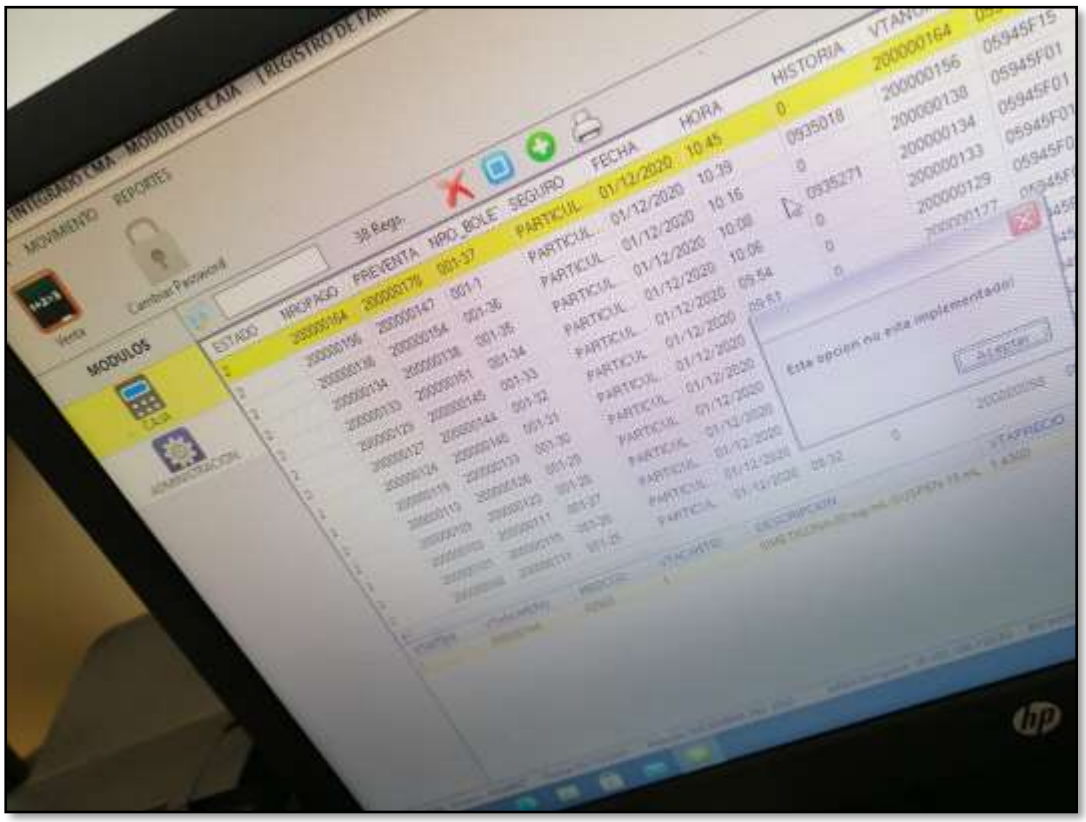


Figura 107. Operando en el sistema de Farmacia del Hospital I

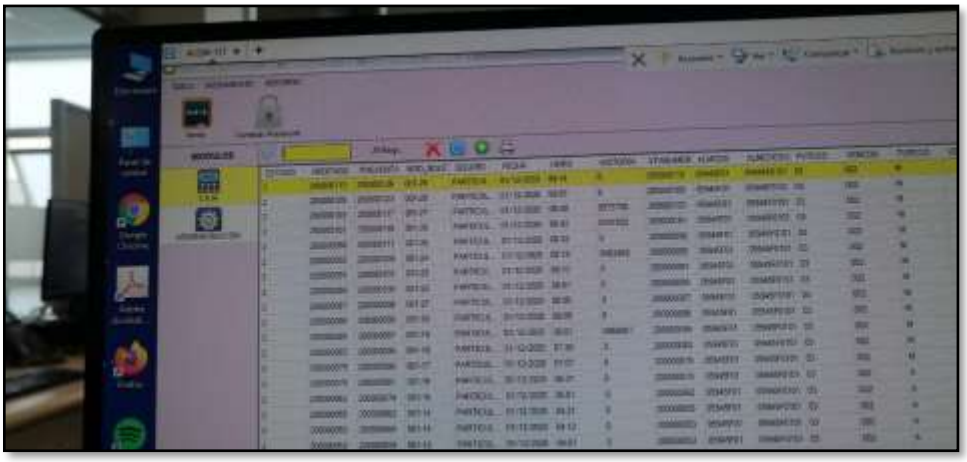


Figura 108. Operando en el sistema de Farmacia del Hospital II

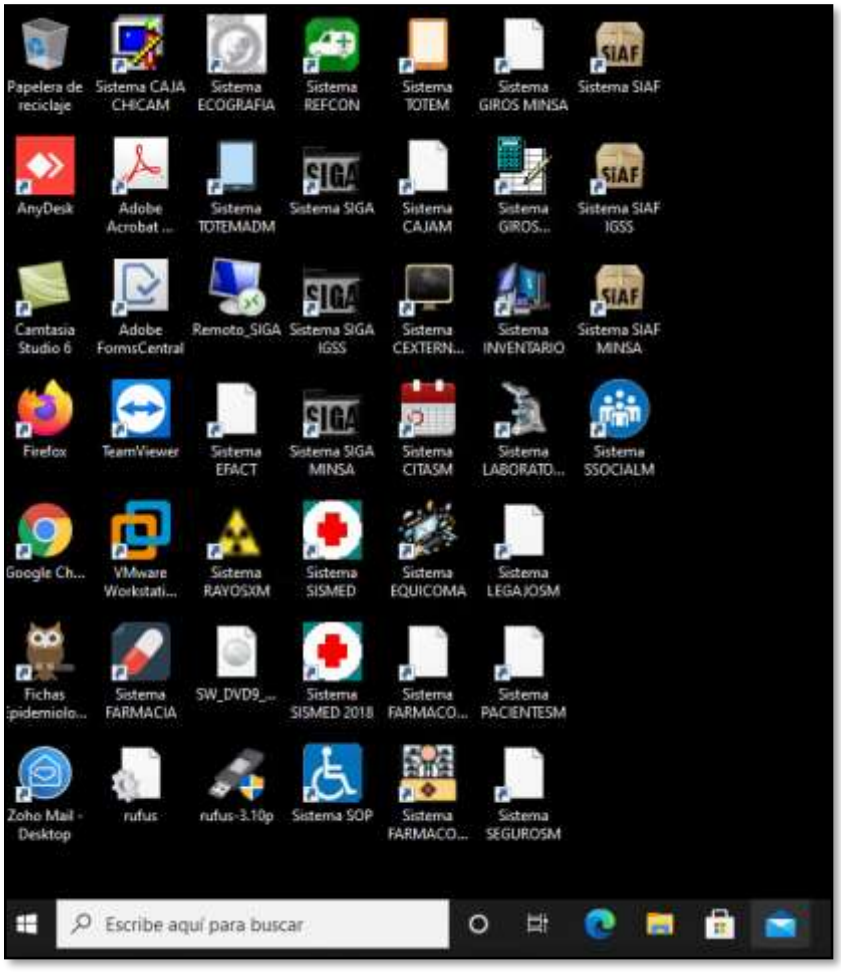


Figura 109. Carga de sistemas y aplicaciones del Hospital según perfil de usuario

Figura 110. Acceso remoto al aplicativo SIGA del MINSA

Figura 111. Acceso remoto al Sistema Médico del Hospital

4.1.3. TERCER RESULTADO:

Se logra monitorear y auditar las conexiones de los trabajadores remotos del Hospital de Vitarte mediante una VPN-SSL a través del Firewall FortiGate-100E.

Para los resultados de este tercer objetivo ya tenemos integrado el FortiAnalyzer con el FortiGate podremos personalizar y exportar reportes de acuerdo a las necesidades de cada área de la entidad.

Demostración – Parte 1: Con ayuda del equipo FortiAnalyzer podremos hacer que todos los logs registrados en el Firewall FortiGate pasen a esta caja de reportes la cual granularmente se encargará de generar reportes personalizados como parte del control y auditoria de las conexiones realizadas por los trabajadores remotos del Hospital de Vitarte.

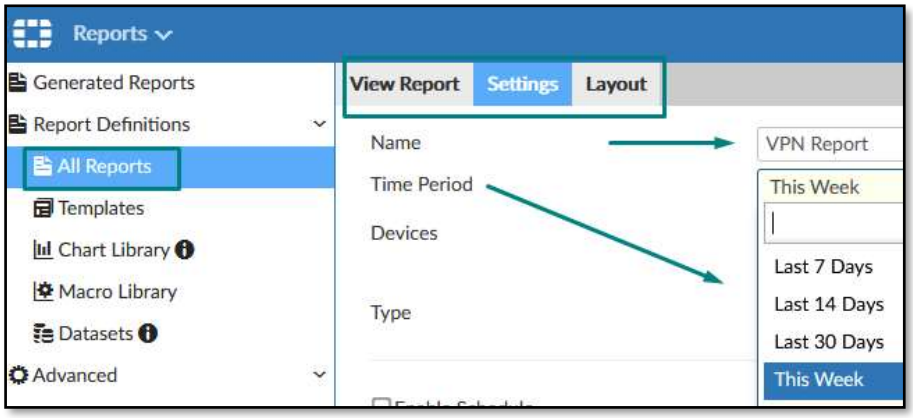


Figura 112. Generando reporte VPN personalizado en FAZ

Demostración – Parte 2: Incluso podremos personalizar los campos de cada reporte agregando ítems como:

- Usuario VPN
- IP publica de donde se realiza la conexión
- IP asignado por el túnel VPN-SSL
- Grupo VPN al cual pertenece el usuario
- Rango de fechas de conexión
- Duración de la conexión (Horas, minutos y segundos)
- Entre otros campos, etc.

Figura 113. Reporte de Auditoria VPN generado por el FAZ en formato PDF

Demostración – Parte 3: Con esta auditoría logramos que las jefaturas de cada unidad midan de acuerdo a estadísticas el trabajo remoto del personal de la entidad, y que las conexiones que establecen los usuarios cumplan los requisitos de cada política de acceso establecida en el Firewall, ya sea por horarios o días según el área administrativa.

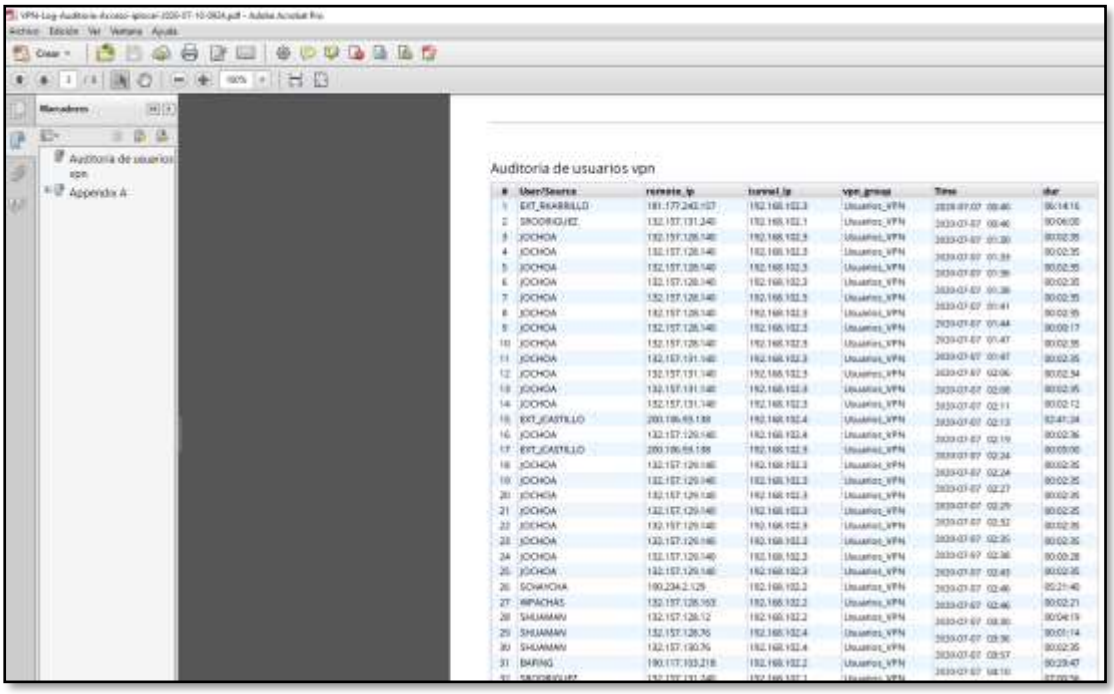


Figura 114. Reporte de conexión detallada por fechas y horas

FORTINET

Acceso de Usuarios VPN - Reporte

#	User/Source	remote_ip	tunnel_ip	vpn_group	Time	dur
1	EXT_CCOCHACHIN	181.177.243.157	192.168.102.7	Usuarios_VPN	2019-09-12 09:48	00:05:11
2	EXT_MRAMOS	191.98.147.246	192.168.102.3	Usuarios_VPN	2019-09-12 11:20	03:29:50
3	BAFING	190.117.103.218	192.168.102.8	Usuarios_VPN	2019-09-12 11:33	00:37:42
4	EXT_FQUISPE	181.65.131.66	192.168.102.7	Usuarios_VPN	2019-09-12 11:44	01:07:30
5	EXT_MLARA	191.98.147.246	192.168.102.6	Usuarios_VPN	2019-09-12 11:47	02:58:30
6	EXT_IVILLALBA	186.18.12.96	192.168.102.7	Usuarios_VPN	2019-09-12 12:55	00:22:05
7	EXT_JCARRO	186.18.12.96	192.168.102.3	Usuarios_VPN	2019-09-12 13:14	01:17:39
8	EXT_BCORTEZM	181.177.243.157	192.168.102.4	Usuarios_VPN	2019-09-12 13:17	04:43:42
9	EXT_BCORTEZM	181.177.243.157	192.168.102.3	Usuarios_VPN	2019-09-12 13:18	00:00:00
10	EXT_MLARA	191.98.147.246	192.168.102.6	Usuarios_VPN	2019-09-12 13:22	01:18:20

Figura 115. Reporte personalizado de Auditoria VPN

4.2.Presupuesto

"Implementación de una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte"

Tabla 8. Presupuesto General del Proyecto

UNIT	DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
GASTOS DE HARDWARE - EQUIPOS DE TELECOMUNICACIONES					
FortiGate-100E	20 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 14 x switch ports), 2 x Shared Media pairs (Including 2 x GE RJ45 ports, 2 x SFP slots).	unidad	1	$ 2,000.00	$ 2,000.00
Licencia FC-10-FG1HE-950-02-DD	Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)	unidad	1	$ 1,300.00	$ 1,300.00
FortiAnalyzer-200D	Centralized log & analysis appliance - 4 x GE RJ45, 4TB storage, up to 100GB/Day of logs.	unidad	1	$ 600.00	$ 1,100.00
Licencia FC-10-L0200-247-02-DD	24x7 FortiCare Contract	unidad	1	$ 400.00	$ 400.00
FortiTokenMobile (Electronic License)	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic license certificate.	unidad	1	$ 3,795.00	$ 3,795.00
GASTO DE RECURSO HUMANO - CONFIGURACION DE INFRAESTRUCTURA Y TECNOLOGÍA					
Encargado de Infraestructura e Implementación	Implementación y participación en las etapas involucradas de la propuesta: - Etapa de Organización (1 MES) - Etapa de Análisis y Diseño (1 MES) - Etapa de Desarrollo e Implementación (1 MES) - Etapa de Operacion y Control (1 MES)	persona	4 meses	$ 2,000.00	$ 8,000.00
TOTAL					**$ 16,595**

CONCLUSIONES

Se concluye que las VPN simbolizan una gran solución para las empresas cumpliendo principios como la seguridad, confidencialidad e integridad de los datos y es tema importante en las organizaciones ante el estado de emergencia sanitaria que cruzamos producto del Covid-19.

Se cumplió con el objetivo general, el cual era implementar una VPN-SSL para mejorar la autenticación y el acceso seguro a los datos en el Hospital de Vitarte todo esto en base a la tecnología Fortinet.

Y por último cumplir precisamente cada objetivo específico del proyecto:

1. Se logra mejorar la autenticación aplicando exitosamente el método de doble factor de autenticación mediante una VPN-SSL para el acceso de los trabajadores remotos del Hospital de Vitarte. Los trabajadores han sido capacitados para la instalación y configuración del aplicativo cliente en sus computadoras (FortiClient) y el aplicativo móvil en sus celulares (FortiToken Mobile).
2. Se consigue disponer de los sistemas, recursos y aplicaciones alojadas en los servidores del Hospital de Vitarte mediante la VPN-SSL LDAP teniendo conexión directa con el dominio como si en sitio se tratase, los usuarios del dominio ya tienen definidos los sistemas de carga en su perfil de acuerdo a su unidad perteneciente. Finalmente, el teletrabajo es puesto en marcha para cada unidad o área del Hospital de Vitarte.
3. Se obtiene monitorear y auditar las conexiones de los trabajadores remotos del Hospital de Vitarte, la integración del FortiAnalyzer con el FortiGate nos permite personalizar y generar reportes de acuerdo a los resultados que el Hospital desea obtener granularmente.

BIBLIOGRAFÍA

Acacio, M. (23 de Octubre de 2020). *Fortinet es líder global en soluciones de ciberseguridad integradas y automatizadas*. Obtenido de https://aslan.es/conociendo-a-fortinet/

Conza, A. (2009). *Diseño e implementación de un prototipo de DMZ y la interconexión segura mediante VPN utilizando el FortiGate 60 (Tesis de Pregrado). Escuela Politécnica Nacional, Facultad de Sistemas.* Ecuador.

De la Cruz, S. (2019). *Implementacion de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo (Tesis de Pregrado). Universidad Nacional Pedro Ruiz Gallo. Facultad de Ciencias.* Perú.

Erazo, P. (2016). *Propuesta de metodología para la implementación de proyectos de redes (Teis de Pregrado). Universidad Católica del Ecuador, Facultad de Ingeniería.* Ecuador.

Espinoza, C. (2018). *Propuesta de una red privada virtual para mejorar el servicio de comunicacion en las tiendas MASS para la empresa Supermercados Peruanos S.A (Tesis de Pregrado). Universidad Autonoma del Perú, Facultad de Ingeniería.* Perú.

Fei, C. (21 de Junio de 2013). *The Research and Implementation of the VPN Gateway Based on SSL.* Obtenido de https://ieeexplore.ieee.org/document/6643282/authors#authors

Fortinet, I. (21 de Marzo de 2021). *Fortinet Latinoamerica - Administración de identidad y acceso*. Obtenido de https://www.fortinet.com/lat/products/identity-access-management

Fortinet, L. (21 de Marzo de 2021). *Fortinet Latinoamerica*. Obtenido de https://www.fortinet.com/

García, L. (19 de Junio de 2016). *Autenticación Multifactor con el uso de un sensor KINECT*. Obtenido de Dialnet: https://dialnet.unirioja.es/servlet/articulo?codigo=5415380

Gonzáles, A. (2006). *Redes Privadas Virtuales (Tesis de Pregrado). Universidad Autonoma del Estado de Hidalgo, Facultad de Ingeniería.* México.

Orosco, B. (2018). *Implementacion y evaluacion de la performance de la comunicacion de voz, video y datos entre las sedes de la UNAJMA mediante una red privada virtual (Tesis de Pregrado). Universidad Nacional José Maria Arguedas, Facultad de Ingeniería.* Perú.

Peña, D. (2016). *Diseño e implementación de una red privada virtual (VPN-SSL) utilizando el metodo de autenticación LDAP en una empresa privada (Tesis de Pregrado). Universidad Central de Venezuela, Facultad de Ingeniería.* Venezuela.

Perdomo, L. (Marzo de 2018). *Diseño de una red privada virtual segura para facilitar la comunicación, trabajo y flujo de información en la empresa QOS LTDA (Tesis de Pregrado). Universidad Cooperativa de Colombia, Facultad de Ingeniería.* Colombia.

Quezada, H. (2016). *Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja.* Loja.

ANEXOS

ANEXO 1

FortiGate 100E Data Sheet

DATA SHEET

FortiGate® 100E Series

FG-100E, FG-101E, FG-100EF, and FG-140E-POE

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway

The FortiGate 100E series provides an application-centric, scalable and secure SD-WAN solution with next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance
- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification
- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking
- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management
- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

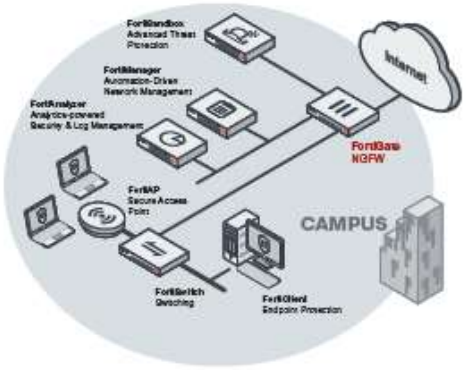
Security Fabric
- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
7.4 Gbps	500 Mbps	360 Mbps	250 Mbps	Multiple GE RJ45, GE SFP Slots | PoE/+ Variants

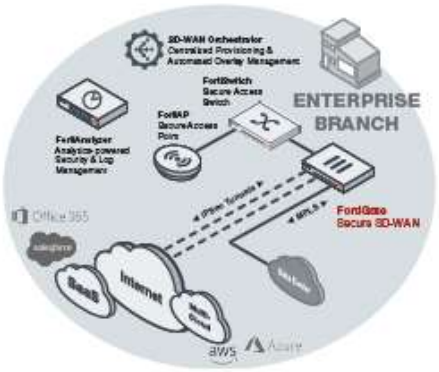
DEPLOYMENT

Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric



Campus Next Generation Firewall Deployment



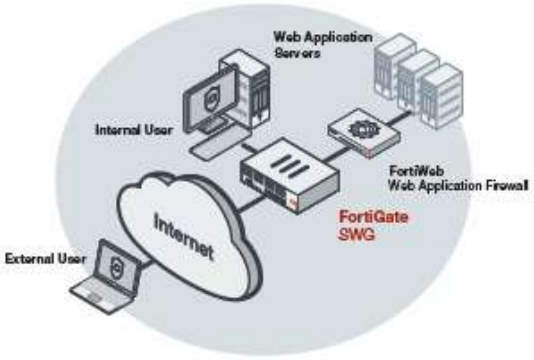
Enterprise Branch Secure SD-WAN Deployment

Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN Orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real- time threat protection

Secure Web Gateway (SWG)

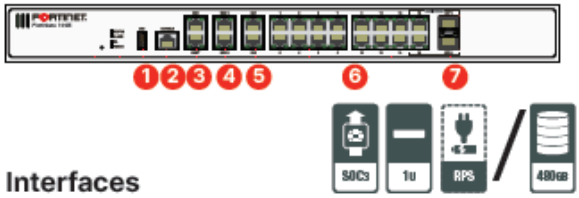
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web



Secure Web Gateway Deployment

HARDWARE

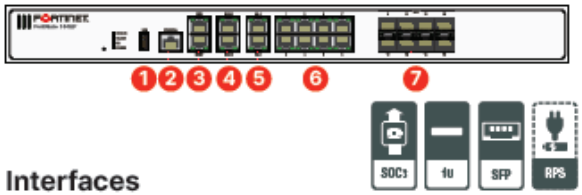
FortiGate 100E/ 101E



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/DMZ Ports
4. 2x GE RJ45 WAN Ports
5. 2x GE RJ45 HA Ports
6. 14x GE RJ45 Ports
7. 2x GE RJ45/SFP Shared Media Pairs

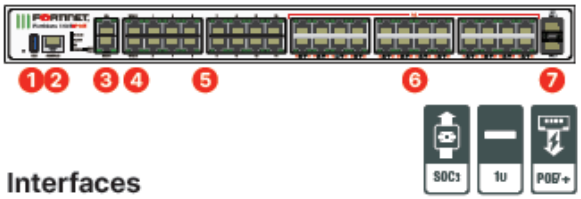
FortiGate 100EF



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/DMZ Ports
4. 2x GE RJ45 WAN Ports
5. 2x GE RJ45 HA Ports
6. 8x GE RJ45 Ports
7. 8x GE SFP Slots

FortiGate 140E-POE



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 24x GE RJ45 POE Ports
7. 2x GE SFP DMZ Slots

Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

Powered by SPU

- Fortinet's custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

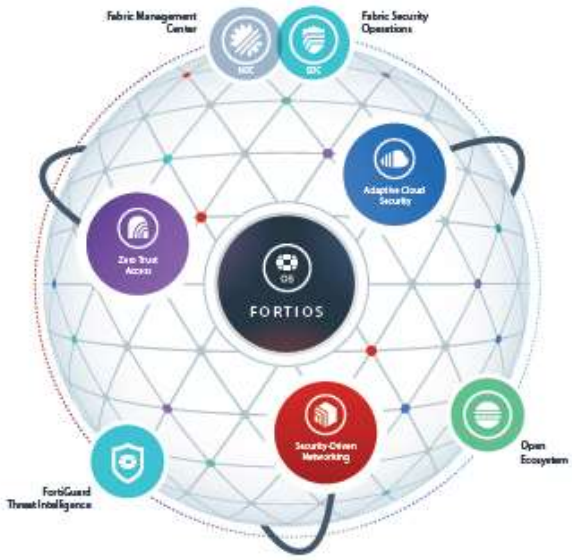
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

	FORTIGATE 100E	FORTIGATE 101E	FORTIGATE 100EF	FORTIGATE 140E-POE
Hardware Specifications				
GE RJ45 Ports	14	14	8	14
GE RJ45 Management/HA/DMZ Ports	1 / 2 / 1	1 / 2 / 1	1 / 2 / 1	1 / 1 / —
GE SFP Slots	—	—	8	2
GE RJ45 PoE/+ Ports	—	—	—	24
GE RJ45 WAN Ports	2	2	2	2
GE RJ45 or SFP Shared Ports	2	2	—	—
USB Port	1	1	1	1
Console Port	1	1	1	1
Internal Storage	—	1× 480 GB SSD	—	—
Included Transceivers	0	0	0	0
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	500 Mbps			
NGFW Throughput [2,4]	360 Mbps			
Threat Protection Throughput [2,5]	250 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	7.4 / 7.4 / 4.4 Gbps			
Firewall Latency (64 byte UDP packets)	3 µs			
Firewall Throughput (Packets Per Second)	6.6 Mpps			
Concurrent Sessions (TCP)	2 Million			
New Sessions/Second (TCP)	30,000			
Firewall Policies	10,000			
IPsec VPN Throughput (512 byte) [1]	4 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	2,000			
Client-to-Gateway IPsec VPN Tunnels	10,000			
SSL-VPN Throughput	250 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	130 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	130			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	125,000			
Application Control Throughput (HTTP 64K) [2]	1 Gbps			
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	32			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	5,000			
High Availability Configurations	Active / Active, Active / Passive, Clustering			
Dimensions and Power				
Height x Width x Length (inches)	1.75 × 17 × 10	1.75 × 17 × 10	1.75 × 17 × 10	1.75 × 17 × 15.5
Height x Width x Length (mm)	44.45 × 432 × 254	44.45 × 432 × 254	44.45 × 432 × 254	44.45 × 432 × 394
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU
Weight	7.28 lbs (3.3 kg)	7.28 lbs (3.3 kg)	7.28 lbs (3.3 kg)	12.4 lbs (5.6 kg)
Power Input	100–240V AC, 50–60 Hz			
Maximum Current	100V / 0.52A, 240V / 0.22A	100V / 0.59A, 240V / 0.25A	100V / 0.52A, 240V / 0.22A	100V / 5A
Total Available PoE Power Budget*	—	—	—	400 W
Power Consumption (Average / Maximum)	23.0 W / 28.6 W; 51.9 VA	24.8 W / 33.8 W; 59.2 VA	24.4 W / 28.6 W; 51.9 VA	477.1 W / 500.0 W
Heat Dissipation	97.6 BTU/h	115.3 BTU/h	97.6 BTU/h	1706.07 BTU/h

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

SPECIFICATIONS

	FORTIGATE 100E	FORTIGATE 101E	FORTIGATE 100EF	FORTIGATE 140E-POE
Operating Environment and Certifications				
Operating Temperature	32–104°F (0–40°C)			
Storage Temperature	-31–158°F (-35–70°C)			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Humidity	10–90% non-condensing			
Noise Level	40.4 dBA	40.4 dBA	40.4 dBA	57 dBA
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6			

ORDERING INFORMATION

Product	SKU	Description
FortiGate 100E	FG-100E	20x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 14x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots).
FortiGate 101E	FG-101E	20 x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 14x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots) 480 GB onboard storage.
FortiGate 100EF	FG-100EF	14x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 8x internal switch ports), 8x SFP ports.
FortiGate 140E-POE	FG-140E-POE	42x GE RJ45 ports (including 2x WAN ports, 1x Mgmt port, 1x HA port, 24x RJ45 GE PoE/PoE+ ports, 14x switch ports), 2x GE SFP DMZ slots.
Optional Accessories		
1 GE SFP LX transceiver module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 transceiver module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX transceiver module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.

BUNDLES

FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE [1]	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video[2] Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard IoT Detection Service	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
Fortinet SOCaaS	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24×7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.0

FORTINET

www.fortinet.com

FG-100E-DAT-R27-20210811

ANEXO 2

FortiToken OTP Data Sheet

DATA SHEET

FortiToken™ One-Time Password Token

Mobile (FTM) One-Time Password (OTP) Application with Push Notification
Hardware Token Time-Based OTP Form-Factors: FTK-200, FTK-200CD and FTK-220

Overview

Fortinet's FortiToken Mobile (FTM) and hardware OTP Tokens (FTK-200, FTK-200CD and FTK-220) are fully integrated with FortiClient, protected by FortiGuard and leverage direct management and use within the FortiGate and FortiAuthenticator security platforms. Secure your network with Fortinet's easy-to-manage, easy-to-use Two-Factor Authentication solutions.

PRODUCT OFFERINGS

FortiToken Mobile

FortiToken Mobile is an OATH compliant OTP generator application for the mobile device supporting both time-based (TOTP) and event-based (HOTP) tokens.

FortiToken 200/200CD

FortiToken 200 is part of Fortinet's broad and flexible two-factor authentication offering. It is an OATH compliant, TOTP. It is a small, keychain-sized device that offers real mobility and flexibility for the end-user.

There is no client software to install; simply press the button and the FortiToken 200 generates and displays a secure one-time password every 60 seconds to verify user identity for access to critical networks and applications. The big LCD screen of the rugged FortiToken 200 is much easier to read than other OTP tokens and there is an indicator on the screen displaying the time left until the next OTP generation. FortiToken 200CD tokens are shipped with an encrypted activation CD for the ultimate in OTP token seed security.

FortiToken 220

The FortiToken 220 OTP token is a mini credit card form factor token. The card is shipped with a precut hole for key ring application. Its sleek and slim design fits neatly into your wallet.

HIGHLIGHTS

Strong Authentication at your Fingertips

It is the client component of Fortinet's highly secure, simple to use and administer, and extremely cost effective two-factor solution for meeting your strong authentication needs. This application makes your Android, iOS and Windows mobile devices behave like a hardware-based OTP token without the hassles of having to carry yet another device. Push notification allows you to view login details on your mobile device to approve or deny with one tap.

Alternatively, you can deploy hardware-based OTP token to prevent users' passwords from stolen, phishing, dictionary and brute-force attacks.

Leverage Existing Fortinet Platforms

Besides offering out-of-the-box interoperability with any time-based OATH compliant authentication server, such as the FortiAuthenticator™ from Fortinet, the FortiToken can also be used directly with the FortiGate® consolidated security platform, including High Availability configurations.

FortiGate has an integrated authentication server for validating the OTP as the second authentication factor for SSL VPN, IPsecVPN, Captive Portal and Administrative login, thereby eliminating the need for the external RADIUS server ordinarily required when implementing two-factor solutions.

Ultra-Secure Token Provisioning

What makes FortiToken mobile OTP application superior to others on the market is that while being simple to use for the end user, and easy to administer and provision for the system administrator, it is actually more secure than the conventional hard token. The token seeds are generated dynamically, minimizing online exposure. Binding the token to the device is enforced and the seeds are always encrypted at rest and in motion.

Online Activation with FortiGuard®

You can activate your FortiToken tokens online directly from FortiGate or FortiAuthenticator using the FortiGuard® Center, which maintains your token seeds in a managed service repository. Once the seeds are activated, they can no longer be accessed from FortiGuard,ensuring that your seeds are safe from compromise. Alternatively, Fortinet also offers an encrypted activation CD solution.

Privacy and Control

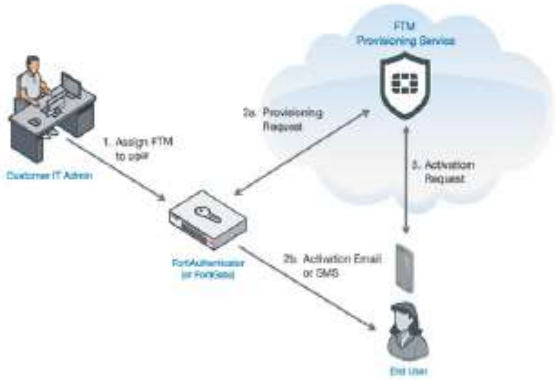
FortiToken Mobile cannot change settings on your phone, take pictures or video, record or transmit audio, nor can it read or sendemails. Further, it cannot see your browser history, and it requires your permission to send you notifications or to change any settings.

And, FortiToken Mobile cannot remotely wipe your phone. Any visibility FortiToken Mobile requires is to verify your OS version to determine app version compatibility. While FortiToken Mobile cannot change any settings without your permission, the following permissions are relevant to FortiToken Mobile operations:

- Access to camera for scanning QR codes for easy token activation
- TouchID/FaceID: used for app security, respectively
- Access to the Internet for communication to activate tokens and receive push notifications
- "Send Feedback by Email", to automatically populate the "Sender" field
- nternally share files between applications to prepare an attachment to be sent by email for "Send Feedback by Email"
- FortiToken must keep the phone awake while it is upgrading the internal database to avoid data corruption

ADVANTAGES

- Unique token provisioning service via FortiGuard™ minimizes provisioning overhead and ensures maximum seed security
- Perpetual token license and unlimited device transfers eliminate annual subscription fees
- Scalable solution leveraging existing end-user devices offers low entry cost and TCO
- Reduces costs and complexity by using your existing FortiGate as the two-factor authentication server
- Zero footprint solution



MAIN FEATURES

FortiToken Mobile

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- Patented Cross Platform Token Transfer
- PIN/Fingerprint protected application
- Copy OTP to the clipboard
- OTP time interval display
- Serial Number display
- Token and app management
- Self-erase brute-force protection
- Apple watch compatibility

FortiToken Hardware Devices

- Integrated with FortiClient™ and protected by FortiGuard
- OATH TOTP compliant
- Large, easy-to-read, LCD display
- Long-life Lithium battery
- Tamper-resistant/tamper-evident packaging

SUPPORTED PLATFORMS

FortiToken Mobile

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10 and Windows Universal Platform
- WiFi-only devices supported (for over-the-air token activation)

FortiToken Hardware Devices

- FortiOS 4.3 and up
- FortiAuthenticator — all versions

Specifications

	FORTITOKEN 200/200CD	FORTITOKEN 220
Onboard Security Algorithm	OATH-TOTP (RFC6238)	OATH-TOTP (RFC6238)
OTP Spec	60 seconds, SHA-1	60 seconds, SHA-1
Component	6-digit high contrast LCD display	Built-in button, 6-character LCD screen, Globally unique serial number
Dimensions (Length x Width x Height)	61.5 x 27.5 x 11.5mm	68 x 38 x 1 mm
Hardware Certification	RoHS Compliant	RoHS, CE, FCC (certificates pending)
Operating Temperature	14–122°F (-10–50°C)	32–122°F (0–50°C)
Storage Temperature	-4–158°F (-20–70°C)	14–140°F (-10–60°C)
Water-Resistant	IP54 (Ingress Protection)	IP54 (Ingress Protection)
Casing	Hard Molded Plastic (ABS) Tamper-Evident	Hard Molded Plastic (ABS) Tamper-Evident
Secure Storage Medium	Static RAM	Static RAM
Battery Type	Standard Lithium Battery	Standard Lithium Battery
Battery Lifetime	3–5 Years	3–5 Years
Customization Available*	Casing Color, Company Logo, Faceplate Branding	Casing Color, Company Logo, Faceplate Branding

* Customizations are quantity based

	FORTITOKEN MOBILE
Onboard Security Algorithm	OATH time and event based OTP generator
OTP Spec	RFC 6238, RFC 4226
Supported Platforms	iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows Phone 8/8.1, Windows 10 and Windows Universal Platform
Over-the-Air Token Activation	WiFi-only devices supported
One-Tap Approval	Login details pushed to phone
PIN/Fingerprint/Facial Security	✓
Serial Number Display	✓
Token and App Management	✓
Self-Erase Brute-Force Protection	✓

PLATFORM SCALABILITY

FortiToken scalability for specific platforms can be found in the Fortinet Product Matrix located at **http://www.fortinet.com/sites/default/files/productdatasheets/Fortinet_Product_Matrix.pdf**

Order Information

Product	SKU	Description
FortiToken Software License Key	FTM-ELIC-5	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5 users. Electronic licence certificate.
	FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic licence certificate.
	FTM-ELIC-20	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 20 users. Electronic licence certificate.
	FTM-ELIC-50	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic licence certificate.
	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic licence certificate.
	FTM-ELIC-200	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic licence certificate.
	FTM-ELIC-500	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 500 users. Electronic licence certificate.
	FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 1000 users. Electronic licence certificate.
	FTM-ELIC-2000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic licence certificate.
	FTM-ELIC-5000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic licence certificate.
	FTM-ELIC-10000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic licence certificate.
FortiToken 200	FTK-200-5	5 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-10	10 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-20	20 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-50	50 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-100	100 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-200	200 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-500	500 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-1000	1000 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-2000	2000 pieces, one-time passwork token, time-based password generator. Perpetual license.
FortiToken 200CD	FTK-200CD-10	FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 10-pack.
	FTK-200CD-20	20 pieces one-time password token, time-based password generator shipped with encrypted seed file on CD. Perpetual license.
	FTK-200CD-50	FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 50-pack.
	FTK-200CD-100	FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 100-pack.
FortiToken 220	FTK-220-5	5 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-10	10 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-20	20 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-50	50 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-100	100 pieces, one-time password token, time-based password generator. Perpetual license.

FORTINET

www.fortinet.com

ANEXO 3

FortiAnalyzer 200D Data Sheet

DATA SHEET

FortiAnalyzer

Security-Driven Analytics and Log Management

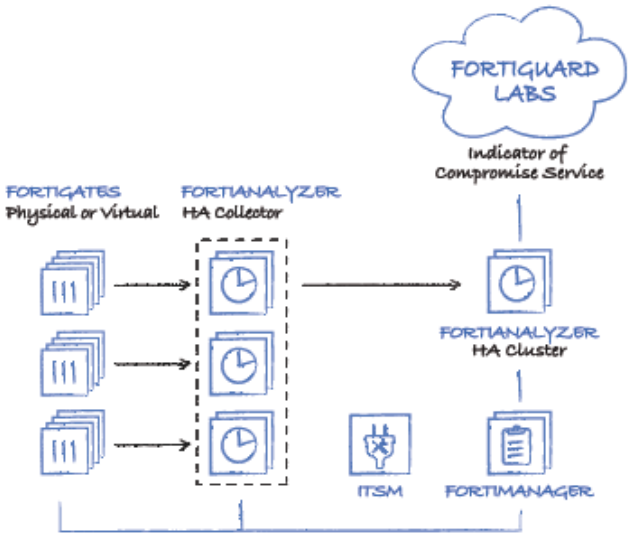
FortiAnalyzer provides deep insights into advanced threats through **Single-Pane Orchestration, Automation, and Response** for your entire attack surface to reduce risks and improve your organization's overall security.

Integrated with **Fortinet's Security Fabric**, FortiAnalyzer simplifies the complexity of analyzing and monitoring new and emerging technologies that have expanded the attack surface, and delivers **end-to-end visibility**, helping you identify and eliminate threats.

Advanced Threat Detection and Correlation allows security and network teams to immediately identify and respond to network security threats across the infrastructure.

Automated Workflows and Compliance Reporting provides customizable dashboards, reports, and advanced workflow handlers for both security and network teams to accelerate workflows and assist with regulation and compliance audits.

Scalable Log Management collects logs from FortiGate, FortiClient, FortiManager, FortiSandbox, FortiMail, FortiWeb, FortiAuthenticator, Generic syslog, and others. Deploy as an individual unit or optimize for a specific operation, and scale storage based on retention requirements.



Key Features

Security Fabric Analytics

- Event correlation across all logs and real-time anomaly detection, with Indicator of Compromise (IOC) service and threat detection, reducing time-to-detect

Fortinet Security Fabric integration

- Correlates with logs from FortiClient, FortiSandbox, FortiWeb, and FortiMail for deeper visibility and critical network insights

Enterprise-grade High Availability

- Automatically back-up FortiAnalyzer databases (up to four node cluster) that can be geographically dispersed for disaster recovery

Security Automation

- Reduce complexity and leverage automation via REST API, scripts, connectors, and automation stitches to expedite security response

Multi-Tenancy and Administrative Domains (ADOMs)

- Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective

Flexible Deployment Options and Archival Storage

- Supports deployment of appliance, VM, hosted, or cloud. Use AWS, Azure, or Google to archive logs as a secondary storage

Feature Highlights

Security Operations Center

FortiAnalyzer's Security Operations Center (SOC) helps security teams protect networks with real-time log and threat data in the form of actionable views, notifications, and reports. Analysts can protect network, web sites, applications, databases, data centers, and other technologies through centralized monitoring, awareness of threats, events, and network activity. The predefined and custom dashboards provide a single-pane-of-glass for easy integration into your Security Fabric. The new FortiSOC service subscription provides built-in incident management workflows with playbooks and connectors to simplify the security analysts' role with enhanced security automation and orchestration.

Incident Detection and Response

FortiAnalyzer's automated incident response capability enables security teams to manage incident life cycle from a single view. Analysts can focus on event management and identification of compromised endpoints through default and customized event handlers with quick detection, automated correlation, and connected remediation of Fortinet devices and syslog servers with incident management and playbooks for quick assignment of incidents for analysis. Track timelines and artifacts with audit history and incident reports, as well as streamline integration with ITSM platforms that help bridge gaps in your Security Operations Center and reinforces your security posture.

FortiAnalyzer Playbooks

FortiAnalyzer Playbooks boost security team abilities to simplify efforts and focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize and automate their investigation use cases to respond to compromised hosts, critical intrusions, blocking C&C IPs, and more. Flexible playbook editor for hosts under investigation. FortiAnalyzer also allows analysts to drill down to a playbook and review task execution details and edit playbooks to define custom processes and tasks. FortiAnalyzer includes built-in connectors for playbooks to interact with other Security Fabric devices like FortiOS and EMS.

Indicators of Compromise

The Indicators of Compromise (IOC) service identifies suspicious usage and artifacts observed on a network or in an operations system that are determined with high confidence to be a computer intrusion. FortiGuard's IOC subscription provides intelligence information to help security analysts identify risky devices and users based on these artifacts. The IOC package consists of around 500K IOCs daily and delivers it via our Fortinet Developers Network (FNDN) to our FortiSIEM, FortiAnalyzer, and FortiCloud products. Analysts can also re-scan historical logs for threat hunting and identify threats based on new intelligence, as well as review users' aggregated threat scores by IP addresses, hostname, group, OS, overall threat rating, a location Map View, and a number of threats.

Asset and Identity

Security Fabric assets and identity monitoring and vulnerability tracking provides full SOC visibility and analytics of the attack surface. Assets and identity visibility and assets classification based on telemetry from NAC. Built-in SIEM module for automated log collection, normalization, and correlation. Integrated with FortiSOAR for further incident investigation and threat eradication. Support export of incident data to FortiSOAR through the FortiAnalyzer Connector and API Admin.

Reports

FortiAnalyzer provides 39+ built-in templates that are ready to use with sample reports to help identify the right report for you. You can generate custom data reports from logs by using the Reports feature. Run reports on-demand or on a schedule with automated email notifications, uploads, and an easy to manage calendar view. Create custom reports with the 700+ built-in charts and datasets that are ready with flexible formats including PDF, HTML, CSV, and XML.

Feature Highlights

SD-WAN Monitoring

SD-WAN dashboards enable customers to instantly see the benefit of applying SD-WAN across multiple WAN interfaces with event handlers to detect SD-WAN alerts for real-time notification and action. History graphs for WAN link health monitoring: Jitter, Latency, Packet Loss, Critical- and High- severity SD-WAN alerts. New Secure SD-WAN report provides an executive summary of important SD-WAN metrics, detailed charts and history graphs for SD-WAN link utilization by applications, latency, Packet Loss, Jitter changes, and SD-WAN performance statistics.

Log Forwarding for Third-Party Integration

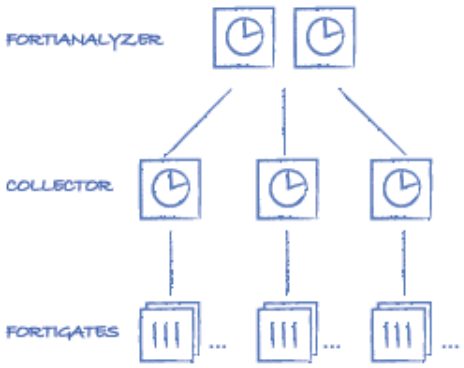
You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or (CEF) server. The client FortiAnalyzer forwards logs to the server FortiAnalyzer unit, syslog server, or CEF server. In addition to forwarding logs to another unit or server, the client retains a local copy of the logs that are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received.

Multi-Tenancy with Flexible Quota Management

Time-based archive / analytic log data policy per Administrative Domain (ADOM), automated quota management based on the defined policy, and trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Mode

You can deploy in Analyzer mode and Collector mode on different FortiAnalyzer units and make the units work together to improve the overall performance of log receiving, analyses, and reporting. When FortiAnalyzer is in Collector mode, its primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. The Analyzer off-loads the log-receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This feature maximizes the Collector's log receiving performance.



Virtual Machines

FortiAnalyzer-VM-S

The new FortiAnalyzer subscription license model consolidates the VM product SKU and the FortiCare Support SKU, as well as IOC and FortiAnalyzer SOC (SOAR/SIEM) services into one single SKU to simplify the product purchase, upgrade, and renewal.

The FortiAnalyzer S-Series SKUs come in stackable 5, 50, and 500 GB/day logs licenses so that multiple units of this SKU can be purchased at a time to increase the number of GB/day logs. This SKU can also be purchased together with other FAZ VM-S SKUs to expand the total number of GB/day logs.

FortiAnalyzer-VM

FortiAnalyzer-VM integrates network logging, analyses, and reporting into a single system, delivering increased knowledge of security events throughout a network. Using virtualization technology, FortiAnalyzer-VM is a software-based version of the FortiAnalyzer hardware appliance and is designed to run on many virtualization platforms. It offers all the features of the FortiAnalyzer hardware appliance.

FortiAnalyzer-VM provides organizations with centralized security event analyses, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analyses of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

FortiAnalyzer Cloud

Fortinet also offers cloud-based analytics and reporting service to enable customers who want to leverage Fortinet managed FortiAnalyzer infrastructure. Customers and partners can easily access their FortiAnalyzer Cloud from their FortiCloud Single-Sign-On Portal.

ANEXO 4

DECRETO SUPREMO N° 017-2015-TR
Ley que regula el teletrabajo

Decreto Supremo que aprueba el Reglamento de la Ley N° 30036, Ley que regula el teletrabajo

DECRETO SUPREMO Nº 017-2015-TR

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, el artículo 23 de la Constitución Política del Perú establece que el trabajo, en sus diversas modalidades, es objeto de atención prioritaria del Estado, el cual protege especialmente a la madre, al menor de edad y al impedido que trabajan;

Que, la Ley N° 30036 regula el teletrabajo como una modalidad especial de prestación de servicios caracterizada por la utilización de tecnologías de la información y las telecomunicaciones, en las instituciones públicas y privadas;

Que, la Cuarta Disposición Complementaria Final de la referida ley dispone que el Ministerio de Trabajo y Promoción del Empleo emita las disposiciones reglamentarias pertinentes mediante decreto supremo;

Que, en tal sentido, corresponde dictar las normas reglamentarias de la Ley N° 30036 que permitan una correcta aplicación de la modalidad de teletrabajo; lo cual beneficiará, además, la empleabilidad de las poblaciones vulnerables;

De conformidad con lo establecido en el numeral 8) del artículo 118 de la Constitución Política del Perú; el artículo 25 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 29381, Ley de Organización y Funciones del Ministerio de Trabajo y Promoción del Empleo; y el Reglamento de Organización y Funciones del Ministerio de Trabajo y Promoción del Empleo, aprobado mediante el Decreto Supremo Nº 004-2014-TR;

DECRETA:

Artículo 1.- Aprobación

Apruébese el Reglamento de la Ley N° 30036, Ley que regula el teletrabajo, que consta de tres (3) Títulos, tres (3) Capítulos, diecisiete (17) artículos, seis (6) Disposiciones Complementarias Finales y una (1) Disposición Complementaria Modificatoria, que forman parte integrante del presente decreto supremo.

Artículo 2.- Refrendo

El presente decreto supremo es refrendado por el Ministro de Trabajo y Promoción del Empleo.

Dado en la Casa de Gobierno, en Lima, a los dos días del mes de noviembre del año dos mil quince.

OLLANTA HUMALA TASSO

Presidente de la República

DANIEL MAURATE ROMERO

Ministro de Trabajo y Promoción del Empleo

REGLAMENTO DE LA LEY N° 30036, LEY QUE REGULA EL TELETRABAJO

TÍTULO PRELIMINAR

Artículo I.- Objeto

El presente decreto supremo tiene por objeto reglamentar la Ley Nº 30036, Ley que regula el teletrabajo. Cualquier mención que se haga a la Ley, debe entenderse que se refiere a dicha norma.

Artículo II.- Ámbito de aplicación

Se encuentran comprendidos dentro del ámbito de aplicación de la Ley y del presente reglamento aquellos trabajadores y servidores civiles que prestan servicios bajo la modalidad de teletrabajo; así como las personas naturales o jurídicas y entidades públicas que los emplean.

La Ley y el presente reglamento serán de aplicación a:

a) Los trabajadores y servidores civiles cuyas labores se ejecuten en el territorio nacional; y

b) Los contratos, resoluciones de incorporación o designación y adendas o acuerdos, por los que se establezca la modalidad de teletrabajo, o el cambio de modalidad presencial por la de teletrabajo y viceversa; suscritos o emitidos en el país.

Artículo III.- Definiciones

Para efectos de la Ley y del presente reglamento, se establecen las siguientes definiciones:

a) Compensación: únicamente para efectos de la Ley y el presente reglamento, se le considera al eventual pago otorgado al teletrabajador al que se refiere el artículo 3 de la Ley y que se efectúa de conformidad con lo señalado en el artículo 10 del presente reglamento.

b) Entidad pública: se entiende por entidad pública a las previstas en el artículo I de la Ley N° 27444, Ley del Procedimiento Administrativo General.

c) Puesto: conjunto de funciones y responsabilidades que corresponden a una posición dentro de una entidad pública, así como los requisitos para su adecuado ejercicio.

d) Servidor civil: servidores de todas las entidades, independientemente de su nivel de gobierno, cuyos derechos se regulan por la Ley N° 30057, Ley del Servicio Civil, por el Decreto Legislativo N° 276, Ley de Bases de la Carrera Administrativa y de Remuneración del Sector Público, por el Decreto Legislativo N° 728, Ley de Productividad y Competitividad Laboral, de carreras especiales y a los contratados bajo el régimen del Decreto Legislativo N° 1057, Decreto Legislativo que regula el régimen especial de contratación administrativa de servicios.

e) SERVIR: Autoridad Nacional del Servicio Civil.

f) Tecnologías de la Información y las Comunicaciones (TIC): conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento y transmisión de información como: voz, datos, texto, vídeo e imágenes.

g) Teletrabajador: trabajador o servidor civil que presta servicios bajo la modalidad de teletrabajo.

h) Teletrabajo: consiste en la prestación de servicios subordinada, sin presencia física en el centro de trabajo o entidad pública, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales, a su vez, se ejerce el control y la supervisión de las labores.

i) Titular de la entidad: máxima autoridad administrativa de una entidad pública.

Artículo IV.- Principios

Son principios que orientan la aplicación de la modalidad de teletrabajo los siguientes:

a) Voluntariedad: el empleador o entidad pública, por razones debidamente sustentadas, puede efectuar la variación de la prestación de servicios a la modalidad de teletrabajo, contando para ello con el consentimiento del trabajador o servidor civil.

b) Reversibilidad: el empleador o entidad pública puede reponer al teletrabajador a la modalidad de prestación de servicios anterior al teletrabajo, si se acredita que no se alcanzan los objetivos bajo la modalidad de teletrabajo.

c) Igualdad de trato: el empleador o entidad pública debe promover la igualdad de trato en cuanto a las condiciones de trabajo de los teletrabajadores, en relación a quienes laboran presencialmente.

d) Conciliación entre la vida personal, familiar y laboral: promover un equilibrio entre las actividades realizadas en los ámbitos, personal, familiar y laboral de los trabajadores o servidores civiles, a través de la modalidad de teletrabajo. En tal sentido, deberá existir una adecuada correspondencia entre la carga de trabajo y la jornada de labores o servicios asignada.

TÍTULO I

DISPOSICIONES APLICABLES AL SECTOR PÚBLICO Y PRIVADO

CAPÍTULO I: PRESTACIÓN DE SERVICIOS BAJO LA MODALIDAD DE TELETRABAJO

Artículo 1.- Requisitos formales del teletrabajo

Los contratos, resoluciones de incorporación o designación y adendas o acuerdos por los que se establezca la modalidad de teletrabajo, o el cambio de modalidad presencial por la de teletrabajo, se celebran por escrito y se sujetan a las condiciones y requisitos previstos por las normas que les sean aplicables, según el régimen al que pertenezca cada

teletrabajador. El empleador o entidad pública debe entregar al teletrabajador un ejemplar de aquellos documentos, según corresponda.

En los documentos antes referidos, el empleador o entidad pública debe consignar, como mínimo, la siguiente información:

a) Los medios informáticos, de telecomunicaciones y análogos a emplearse para la prestación del servicio, así como la parte del contrato responsable de proveerlos.

b) En caso los medios sean proporcionados por el empleador o entidad pública, debe indicarse las condiciones de utilización, las responsabilidades del teletrabajador sobre los mismos y el procedimiento de devolución al momento de finalizar la modalidad de teletrabajo, de corresponder.

c) En caso los medios sean proporcionados por el teletrabajador, debe indicarse el monto de la compensación que deberá efectuar el empleador; en caso de entidades públicas, dicho pago se realizará conforme al marco legal vigente.

d) Las medidas sobre la gestión y seguridad de la información derivadas del uso de los medios con que se preste el servicio bajo la modalidad de teletrabajo.

e) La jornada que se asigne al teletrabajador, de acuerdo con los límites previstos en las normas que resulten aplicables.

f) El mecanismo de supervisión o de reporte a implementarse para facilitar el control y supervisión de las labores, de ser el caso.

Cuando se trate de un cambio de la modalidad convencional a la modalidad de teletrabajo, el empleador o entidad pública debe indicar la justificación del cambio así como los objetivos que persigue con aquella variación.

La entrega al teletrabajador de medios informáticos, de telecomunicaciones y análogos, adicionales a los inicialmente proporcionados por el empleador o entidad pública, deberá constar por escrito, detallándose los bienes entregados. La constancia se suscribe por ambas partes y se emite por duplicado.

Durante el desarrollo del teletrabajo, las partes pueden acordar la modificación de los términos inicialmente pactados, de conformidad con las normas vigentes, respetando la información mínima señalada en el presente artículo.

Artículo 2.- Formas de teletrabajo

La modalidad de teletrabajo puede desarrollarse bajo las siguientes formas:

a) Forma completa: el teletrabajador presta servicios fuera del centro de trabajo o del local de la entidad pública; pudiendo acudir ocasionalmente a estos para las coordinaciones que sean necesarias.

b) Forma mixta: el teletrabajador presta servicios de forma alternada dentro y fuera del centro de trabajo o local de la entidad pública.

No se considera teletrabajador al trabajador o servidor civil que ocasionalmente presta servicios fuera del centro de trabajo o entidad pública.

Artículo 3.- Jornada de trabajo o de servicio

La jornada ordinaria de trabajo o de servicio que se aplica al teletrabajo, se sujeta a los límites previstos en las normas sobre la materia.

De conformidad con el régimen que corresponda, los trabajadores y servidores civiles pueden prestar servicios bajo la modalidad de teletrabajo en jornadas a tiempo parcial o en sistemas de media jornada, respectivamente, de acuerdo con los límites y requisitos previstos en las normas correspondientes, solo si éstos se encuentran sujetos a fiscalización inmediata de la jornada.

Las exclusiones a la jornada máxima de trabajo o de servicio previstas en las normas que regulan la jornada de trabajo en los sectores público y privado se aplican al teletrabajo.

Artículo 4.- De la variación de la modalidad de prestación de servicios y su reversión

4.1 La variación de la modalidad convencional de prestación de servicios a la de teletrabajo es voluntaria y no puede significar en sí misma la afectación de la naturaleza del vínculo entre el teletrabajador y la entidad pública o el empleador, de los derechos, beneficios, categoría y demás condiciones del trabajador o servidor civil, salvo aquellas vinculadas a la asistencia al centro de trabajo o local de la entidad pública.

4.2 El acuerdo de variación de la modalidad convencional de prestación de servicios a la de teletrabajo y viceversa, puede ser permanente o sujeta a plazo determinado.

4.3 La reversión del teletrabajo a la modalidad convencional se sujeta a las siguientes reglas:

a) Procede por acuerdo escrito entre las partes. El empleador o entidad pública debe entregar al teletrabajador una copia del acuerdo de reversión.

b) Procede por decisión unilateral del empleador o entidad pública, la que es comunicada por escrito al teletrabajador en un plazo razonable no menor de quince (15) días naturales de anticipación, más el término de la distancia. Para que opere la reversión, el empleador o entidad pública debe sustentar en dicha comunicación que no se han alcanzado los objetivos de la actividad en la modalidad de teletrabajo.

c) Cuando el teletrabajador solicita la reversión, el empleador o entidad pública puede denegar dicha solicitud en uso de su facultad directriz. La respuesta a la solicitud del teletrabajador debe sustentarse y comunicarse por escrito en un plazo no mayor a seis (06) días naturales. En caso la respuesta sea afirmativa, ésta debe indicar la fecha de retorno al centro de trabajo o local de la entidad pública.

d) Procede cuando se cumple el plazo previsto en el acuerdo de variación.

4.4. En caso el trabajador o servidor civil inicie su vínculo en la modalidad de teletrabajo, la variación a la modalidad convencional de prestación de servicios y su reversión siguen las mismas reglas previstas en los numerales anteriores.

Artículo 5.- Cuestionamientos a la variación de modalidad y su reversión

El trabajador, servidor civil o teletrabajador que cuestione la variación de la modalidad de prestación de servicios o su reversión pueden impugnar la decisión del empleador o entidad pública conforme a las normas aplicables al régimen al que pertenezcan.
Sin perjuicio de ello, en caso se presente cualquiera de los supuestos de actos de hostilidad equiparables al despido durante el desarrollo de la modalidad de teletrabajo, el teletrabajador sujeto al régimen laboral de la actividad privada puede accionar conforme a los artículos 30 y 35 del Texto Único Ordenado del Decreto Legislativo Nº 728, Ley de Productividad y Competitividad Laboral, aprobado por el Decreto Supremo N° 003-97-TR.

CAPÍTULO II: DERECHOS Y OBLIGACIONES DEL TELETRABAJADOR

Artículo 6.- Derechos y beneficios del teletrabajador

El teletrabajador tiene los mismos derechos y beneficios que los trabajadores que prestan servicios bajo la modalidad convencional, de acuerdo al régimen al que pertenezca cada teletrabajador, salvo aquellos vinculados a la asistencia al centro de trabajo. Entre los derechos que serán garantizados se encuentran:

a) Capacitación sobre los medios informáticos, de telecomunicaciones y análogos que emplearán para el desempeño de la ocupación específica, así como sobre las restricciones en el empleo de tales medios, la legislación vigente en materia de protección de datos personales, propiedad intelectual y seguridad de la información. La capacitación se realiza antes de iniciarse la prestación de servicios bajo la modalidad de teletrabajo y cuando el empleador introduzca modificaciones sustanciales a los medios informáticos, de telecomunicaciones y análogos con los que el teletrabajador presta sus servicios.

b) Intimidad, privacidad e inviolabilidad de las comunicaciones y documentos privados del teletrabajador, considerando la naturaleza del teletrabajo.

c) Protección de la maternidad y el periodo de lactancia de la teletrabajadora.

d) Seguridad y salud en el trabajo, en lo que fuera pertinente y considerando las características especiales del teletrabajo.

e) Libertad sindical, de acuerdo al régimen que resulte aplicable. En ningún caso, la aplicación o el cambio de modalidad de prestación de servicios de un trabajador o servidor civil a la modalidad de teletrabajo podrá afectar el ejercicio de sus derechos colectivos.

Artículo 7.- Obligaciones del teletrabajador

El teletrabajador tendrá las mismas obligaciones que los trabajadores y servidores civiles que prestan servicios bajo la modalidad convencional para el empleador o entidad pública,

conforme al régimen que resulte aplicable. Entre estas obligaciones, se encuentran las siguientes:

a) Cumplir con la normativa vigente sobre seguridad de la información, protección y confidencialidad de los datos y seguridad y salud en el trabajo.

b) Durante la jornada de trabajo o servicio, el teletrabajador deberá estar disponible para las coordinaciones con el empleador o entidad pública, en caso de ser necesario.

c) Guardar confidencialidad de la información proporcionada por el empleador o entidad pública para la prestación de servicios.

d) Cuando al teletrabajador le sean suministrados por parte del empleador o la entidad pública los elementos y medios para la realización de las labores, estos no podrán ser usados por persona distinta al teletrabajador, quien, salvo pacto en contrario, deberá restituir los objetos entregados en buen estado al final de esta modalidad, con excepción del deterioro natural.

CAPÍTULO III: OTRAS DISPOSICIONES

Artículo 8.- Aplicación del teletrabajo a favor de las poblaciones vulnerables

En la medida de lo posible, y siempre que cumplan con los requisitos para el puesto, el empleador o entidad pública dará preferencia a las poblaciones vulnerables para que puedan prestar servicios bajo la modalidad de teletrabajo, de conformidad con las normas vigentes.

En ese marco, y sin perjuicio de otras medidas que pueda adoptar conforme a lo señalado en el presente artículo, el empleador o entidad pública evaluará la aplicación de la modalidad de teletrabajo para garantizar el cumplimiento de la cuota de empleo de las personas con discapacidad, de conformidad con la Ley N° 29973; así como para garantizar la continuidad de la prestación del servicio de trabajadoras y servidoras civiles gestantes y lactantes, trabajadores y servidores civiles responsables del cuidado de niños, adultos mayores, personas con discapacidad, o familiares directos que se encuentren con enfermedad en estado grave o terminal o sufran accidente grave.

Artículo 9.- Responsabilidades de las partes por los medios a emplearse para el teletrabajo

9.1 La provisión de las condiciones de trabajo para la prestación del teletrabajo, tales como equipos, acceso a internet, conexiones de red, programas informáticos, medidas de seguridad de la información, entre otros, obliga a quien los otorga a garantizar la idoneidad de los mismos.

9.2 Si el empleador o entidad pública no cumple con entregar las condiciones de trabajo cuando le corresponda, pese a que el teletrabajador está a disposición para prestar el servicio, aquél no podrá dejar de reconocer la remuneración a la que el teletrabajador tiene derecho; salvo norma legal en contrario.

9.3 En casos de pérdida, sustracción, deficiencia o deterioro, que haga imposible el uso de las condiciones de trabajo, por causas no imputables a ninguna de las partes, el teletrabajador deberá informar de inmediato al empleador o entidad pública con la finalidad de que adopte medidas para garantizar la continuidad de las labores. En tales casos, el teletrabajador tendrá derecho al reembolso de los gastos autorizados en que incurra para asegurar la continuidad de la prestación de servicio, salvo norma legal en contrario. Si las condiciones de trabajo fueron otorgadas por el empleador o entidad pública, el teletrabajador sólo es responsable por aquello que le sea atribuible.

9.4 En los casos previstos en el numeral anterior, cuando pese a las medidas adoptadas resulte imposible la prestación del servicio, el empleador o entidad pública puede acordar la prestación de servicios en la modalidad convencional mientras dure la imposibilidad, conforme a lo establecido en el numeral 4.2 del artículo 4 del presente reglamento.

Artículo 10.- Pago por los medios aportados por el teletrabajador

El pago de la compensación por las condiciones de trabajo asumidas por el teletrabajador, que debe efectuar el empleador o entidad pública, al que se refiere el segundo párrafo del artículo 3 de la Ley, se sujeta a lo siguiente:

a) Para el caso del sector privado, la compensación se realiza en dinero y en moneda de curso legal. El monto se determina por acuerdo de las partes. A falta de acuerdo, éste se determina en función al valor de los bienes en el mercado.

b) Para el caso del sector público, el referido pago que pudiese realizarse cuando fuese el caso, está sujeto a las disposiciones de carácter presupuestal aplicables a las entidades de dicho sector.

Artículo 11.- Carácter no remunerativo de las condiciones provistas por el empleador

Los bienes y servicios brindados por el empleador o entidad pública como condiciones de trabajo no tienen carácter remunerativo para ningún efecto legal.

TÍTULO II

DISPOSICIONES ESPECIALES APLICABLES AL SECTOR PÚBLICO

Artículo 12.- Teletrabajo en el sector público

Sin perjuicio de lo establecido en la cuarta disposición complementaria final del presente reglamento, las entidades públicas se encuentran facultadas para aplicar la modalidad de teletrabajo cuando así lo requieran sus necesidades.

Artículo 13.- Aprobación de la modalidad de teletrabajo en las entidades públicas

Las entidades públicas identificarán progresivamente aquellos puestos que puedan desempeñarse a través de la modalidad de teletrabajo, en el marco de sus instrumentos de gestión aprobados.

Asimismo, el titular de la entidad aprobará el informe que establezca, en razón de las características del puesto, cuáles de ellos pueden desempeñarse a través de la modalidad de teletrabajo.

Para ello se constituirá una Comisión de Teletrabajo, en la cual participen un representante de la Oficina de Recursos Humanos, de la Oficina General de Administración, de la Oficina de Tecnología de la Información y del Titular de la entidad.

La Comisión de Teletrabajo tiene como función elaborar una propuesta de puestos identificados en la entidad pública que pueden desempeñarse a través de la modalidad de teletrabajo.

Artículo 14.- Aplicación de la modalidad de teletrabajo

La aprobación de la variación a la modalidad de teletrabajo de un servidor civil se llevará a cabo mediante un informe del Responsable de la Oficina de Recursos Humanos o el que haga sus veces, previa solicitud del jefe inmediato. La solicitud puede ser de oficio o como consecuencia del pedido formulado por un servidor civil.

Artículo 15.- Situaciones excepcionales para la modalidad de teletrabajo

Las entidades públicas pueden requerir la contratación de servidores civiles que se desempeñen como teletrabajadores desde un inicio de la prestación de servicios, bajo los siguientes supuestos:

a) En circunstancias de caso fortuito o fuerza mayor que requieran que algunas actividades se realicen bajo la modalidad de teletrabajo.

b) Cuando se afecte la prestación de servicios de manera imprevista, y para garantizar su continuidad se pueda realizar algunas actividades bajo la modalidad de teletrabajo.

c) Cuando se produce el incremento extraordinario y temporal de actividades en una determinada entidad.

Artículo 16.- Capacitación a los servidores civiles

Las entidades públicas deben considerar en la planificación de las necesidades de capacitación de sus servidores civiles, actividades vinculadas a los siguientes temas:

a) Competencias para que los servidores civiles se puedan desempeñar en la modalidad de teletrabajo.

b) Lineamientos y políticas generales de la organización para el teletrabajo.

c) Prevención en salud y riesgos laborales.

d) Uso y manejo de las herramientas de tecnología de la información y la comunicación.

Artículo 17.- Competencia de SERVIR

En el marco de sus competencias, SERVIR emite las disposiciones complementarias que desarrollen las materias previstas en el presente Título, así como otras que contribuyan a la implementación de la modalidad de teletrabajo en el sector público.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Difusión de la normativa y promoción del teletrabajo

El Ministerio de Trabajo y Promoción del Empleo y los gobiernos regionales desarrollan actividades de difusión de la normativa aplicable al teletrabajo, así como de promoción para su progresiva implementación en el ámbito privado, brindando servicios de información, orientación y asesoría.

Segunda.- Registro en Planilla Electrónica

El empleador y la entidad pública registran en la Planilla Electrónica la condición de teletrabajador en la modalidad completa o mixta aplicada, y otros criterios que se establezcan mediante Resolución Ministerial.

Tercera.- Informe anual de la implementación del teletrabajo

El Ministerio de Trabajo y Promoción del Empleo, a través de la Dirección General de Promoción del Empleo, elabora un informe anual sobre los resultados de la implementación del teletrabajo en el ámbito privado.

Cuarta.- Cuota mínima de teletrabajo en el sector público

En concordancia con la Primera Disposición Complementaria Final de la Ley, SERVIR definirá la cuota mínima de puestos en las entidades del sector público a los que se aplicará el teletrabajo, en un plazo de ciento ochenta (180) días hábiles contados a partir de la publicación del presente reglamento.

Quinta.- Actuación de la Inspección del Trabajo

El Sistema de Inspección del Trabajo del Sector Trabajo y Promoción del Empleo orienta y fiscaliza el cumplimiento de las normas contenidas en la Ley y el presente Reglamento en los centros de trabajo, locales de entidades públicas y, en general, los lugares en que se ejecute la prestación laboral, siempre que el empleador o entidad pública esté sujeto al régimen laboral de la actividad privada.

Sexta.- Normas complementarias

Mediante resolución ministerial, el Ministerio de Trabajo y Promoción del Empleo, en un plazo de noventa (90) días hábiles contados a partir de la publicación del presente reglamento, emite las disposiciones complementarias que resulten necesarias para la mejor aplicación del presente decreto supremo en el marco de la actividad privada, en particular, en materia de control de asistencia, seguridad y salud en el trabajo, entre otras.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

Única.- Modificación del Reglamento de la Ley General de Inspección del Trabajo

Incorpórense los numerales 24.16, 24.17, 24.18 y 24.19 al artículo 24 del Reglamento de la Ley General de Inspección del Trabajo, aprobado por Decreto Supremo N° 019-2006-TR, los que quedarán redactados de la siguiente forma:

"Artículo 24.- Infracciones graves en materia de relaciones laborales

Son infracciones graves, los siguientes incumplimientos:

[...]

24.16. Aplicar el cambio de modalidad de un trabajador convencional a la modalidad de teletrabajo o viceversa sin su consentimiento.

24.17 Aplicar la reversión sin cumplir con los requisitos establecidos por ley.

24.18 No cumplir con las obligaciones referidas a la capacitación del teletrabajador previstas en las normas de la materia.

24.19 No cumplir con el pago de la compensación por las condiciones de trabajo asumidas por el teletrabajador.

ANEXO 5

ACTA DE CIERRE DEL PROYECTO

ACTA DE CIERRE N.º 08-2020-UEI/HV

A : **Bach. Roberto Flores Ayqui**
Tercero – Analista y Administrador de Red

ASUNTO : Entrega de Acta de cierre - Implementación de Tecnología Fortinet VPN-SSL - 2020

FECHA : Vitarte,25 de junio del 2020

Es grato dirigirme a usted para saludarle cordialmente y al mismo tiempo informarle lo siguiente:

ANTECEDENTE

Resolución Directoral N°228-2020-D/HV, que aprueba el Plan Operativo Institucional 2020 modificado V.02 del Hospital Vitarte.

Decreto Supremo N°024-2019-SA, establecen medidas de mejora de la prestación de servicios de salud a ser implementadas de manera progresiva y a nivel nacional.

Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

DECLARACION DE ACEPTACION Y COMPROMISO

La unidad de Estadística e informática del hospital de vitarte otorga la presente acta de finalización de las etapas y/o actividades del proyecto **Implementación y configuración de la Tecnología Fortinet y solución VPN-SSL para la modalidad de Teletrabajo**, de esta manera se cubre las necesidades y exigencias de cada una de las áreas y/o servicios de la institución.

Etapas		Tiempo
Item	Descripción	
1	Etapa de Organización	1 mes
2	Etapa de Análisis y Diseño	1 mes
3	Etapa de Desarrollo e Implementación	1 mes
4	**Etapa de Operación y Control**	**1 mes**

CONCLUSION

Por lo tanto, se considera la participación a lo largo del proyecto y el logro de los objetivos para las diversas unidades del hospital de vitarte correspondiente al año 2020.

Sin otro particular, es propicia la oportunidad para reiterar las muestras de mi especial consideración y estima personal.
Atentamente,

MINISTERIO DE SALUD
HOSPITAL VITARTE
Sr. Luis Vladimir Pilco Arco
JEFE DE LA UNIDAD DE ESTADISTICA E INFORMATICA

C.c.
VPA/jclbr